Second Edition

Information Lifecycle Governance Leader Reference Guide

A Model for Improving Information and eDiscovery Economics with Information Lifecycle Governance

CGOC

"The best way to reduce the amount of data — delete it."

— Sheila Childs, Research Vice President, Gartner

A publication of the Compliance, Governance & Oversight Council, 2014

Contents

Introduction

Data is growing at unprecedented rates, yet the processes for communicating exactly what amongst this information glut is essential to the business haven't kept pace with the complexity and volume of the changing landscape. As the gap between the value of information and its associated costs and risks continues to expand, companies must get serious about improving their information economics.

Adopting an Information Lifecycle Governance (ILG) approach is central to achieving success with information economics. By following a proven roadmap of ILG tools and processes, organizations can foster the transparency that aids in the defensible disposal of excessive data. By getting rid of unnecessary data debris, everyone wins. Business users will gain optimal value from corporate information assets, IT and legal departments will be able to maintain tighter controls over costs, and organizations greatly lower their overall exposure to risk.

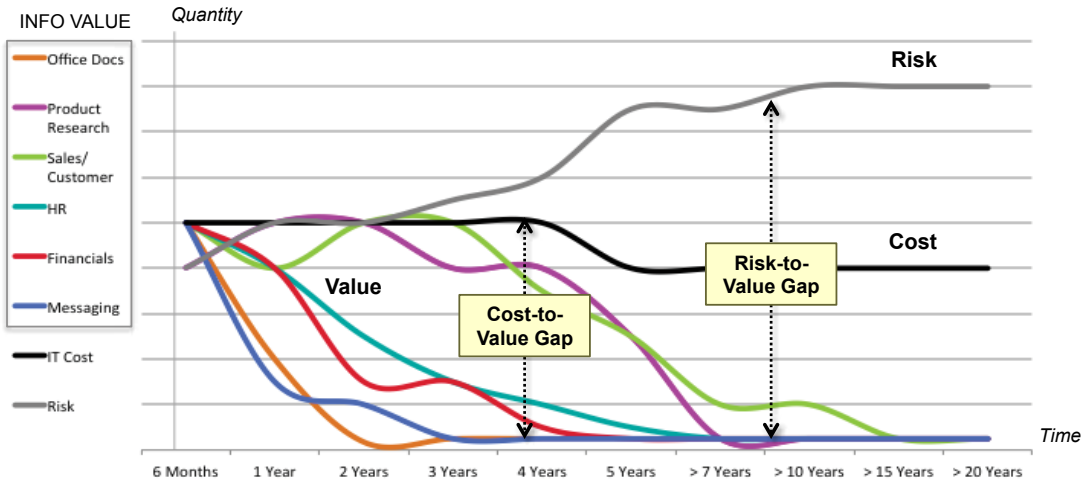
The value proposition around information economics is all the more crucial today given that data is pouring in from virtually every corner of the organization, in a variety of formats--from social media, email, and video content to e-commerce and other Web-based transactions. While some of the incoming data can be parlayed into insights that facilitate more effective decision making, the lion's share of organizational content carries substantial risk without delivering measurable benefit to the business.

It's no longer about one thing

Volume	Velocity	Variety
12 terabytes	**5** million	**4** terabytes/site/day
of Tweets create daily	trade events per second	average surveillance video
Analyze product sentiment	Identify potential fraud	Monitor events of interest
15 petabytes	**500** million	**80%** info growth
of new information daily	call detail records per day	is unstructured content …
Determine relevance	Prevent customer churn	Improve customer satisfaction

The numbers paint a telling picture: Only 1% of enterprise information is subject to legal hold, 5% is related to regulatory record keeping, and 25% has real business utility. So what about the remaining 69% of the information deluge? It is of questionable value to the organization, yet storing and managing the information greatly escalates costs and increases an organization's exposure to a variety of risks. As a result, companies have little to gain—and actually much more to lose--by indiscriminately holding onto data simply because of their inability to properly link actual demand for it to an ever-widening reservoir of information assets.

Information Value Declines Over Time, Cost and Risk Don't



Disconnected stakeholder processes and the existing silos between IT, legal, business, security, and Records Information Management (RIM) make it difficult to achieve the transparency that is crucial to knowing what data is an asset and what constitutes debris. RIM and legal, for example, are well aware of their regulatory and legal duties for information, but they don't actively know where the relevant information resides. Business knows the value of information, but is not necessarily cognizant of its cost to the enterprise. IT knows where all the information resides, but isn't fully mindful of the legal duties, business value, or duration of its needs. With data volume overwhelming traditional information governance processes, these disconnects lead to operational challenges. In turn they contribute to risks such as complexity in applying legal holds, inefficiencies in data management, and difficulties aligning IT with business.

Company executives and Information Lifecycle Governance leaders are actively working to define and operationalize ILG programs and improve processes to address these challenges and achieve cost and risk reduction benefits. Central to enterprise ILG initiatives are formalizing processes around:

Value-Based Archiving & Defensible Disposal

- Archive to shrink storage, align cost to value
- Dispose rather than store unnecessary data

Extend and automate retention management

- Include electronic data that has business value in addition to records for regulatory requirements
- Automate retention schedules across all information to enable reliable, systematic disposal

Automate the legal holds and ediscovery process

- Structure and automate legal holds process to lower risk, increase precision, enable disposal
- Analyze in place to reduce unnecessary collection, processing and review

Three critical inflection points in information lifecycle drive value, cost, and risk:

1. Analytics to maximize value as context erodes
2. Archiving and tiering to ensure cost reductions as value declines
3. Disposal to ensure that when need is gone, there is no remaining cost

Information Lifecycle Governance improves information economics for legal, business, & IT

Leverage information for better decisions

Don't waste budget on unnecessary IT or legal services

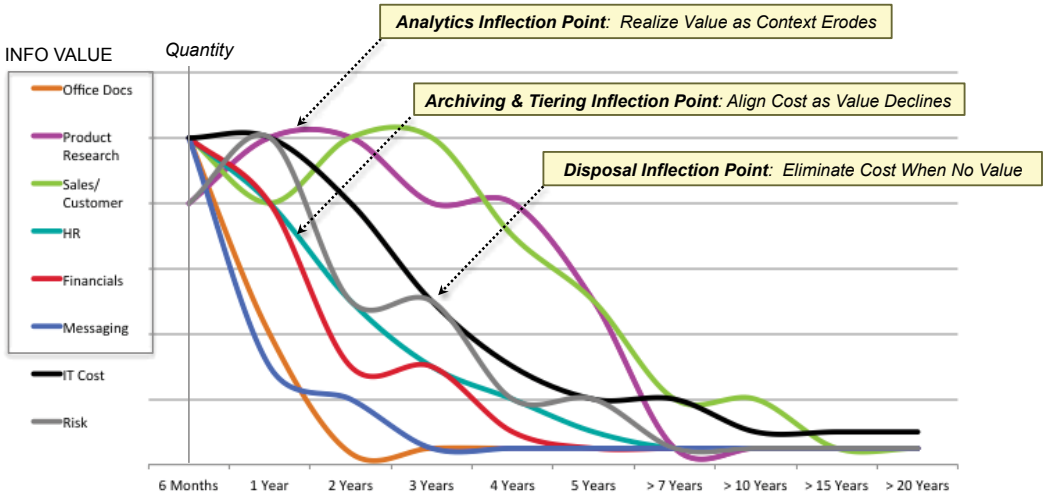
Meet e-discovery obligations cost effectively and efficiently for the enterprise

Manage conflicting privacy and regulatory duties

Minimize "run the shop" costs to increase investment in "grow the firm" activities

Cut total costs even as total volume rises

ILG Policy-Driven Alignment of Information Cost to Value



While spot "clean up" projects can be helpful, they don't go far enough in addressing the broader issues around defensible disposal, especially in an era of high-octane data growth. Instead, companies need to take a systematic approach to ILG, optimizing 18 processes that instrument defensible disposal into the fabric of information management and as a result, improve information economics. Organizations with a high level of maturity in these 18 ILG processes are much more likely to understand and extract information value, align cost to value over time, minimize information and legal risks, and lower total IT and legal costs.

This CGOC ILG Leaders' Guide serves as a roadmap to improving information economics via the implementation of an effective ILG program, including the optimization of 18 processes that have been peer reviewed by the 2,400-member CGOC community. The Guide will help members:

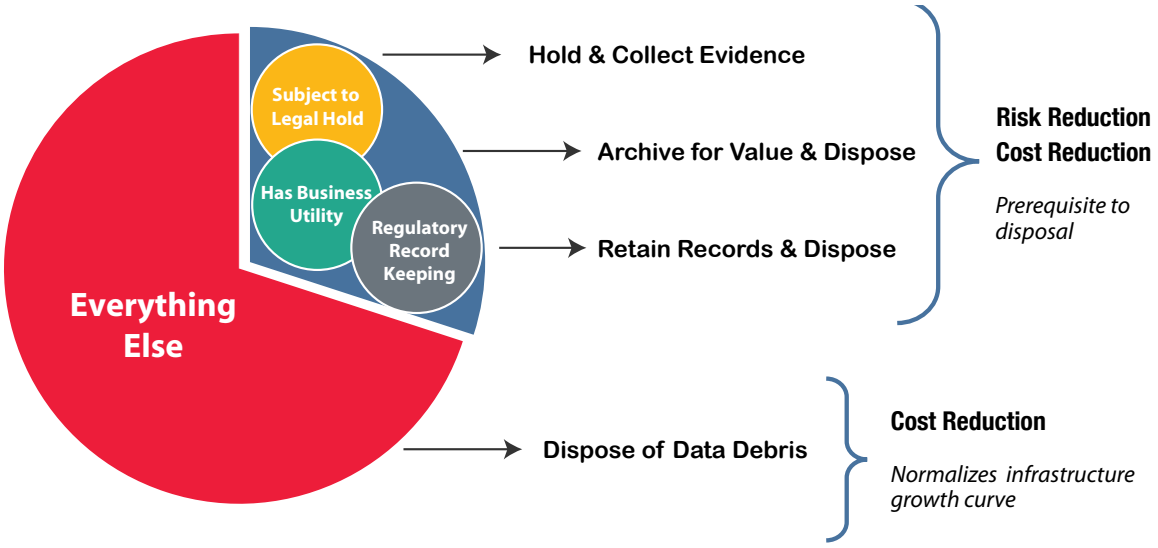
- Define the economic and business objectives of an information governance program to quantify savings and ensure appropriate funding for change
- Establish a program strategy
- Structure an organization that aligns functional silos to ensure savings and business objectives are achieved
- Identify and improve the business processes for defensible disposal and risk reduction
- Audit these processes to ensure systemic, sustainable change

We trust you'll find this ILG Leaders' Guide a useful tool for achieving defensible disposal and in turn, making headway on improving information economics. Please continue to contribute to the dynamic CGOC community as you lead and learn.

Defining Program Strategy

Strategic Focus

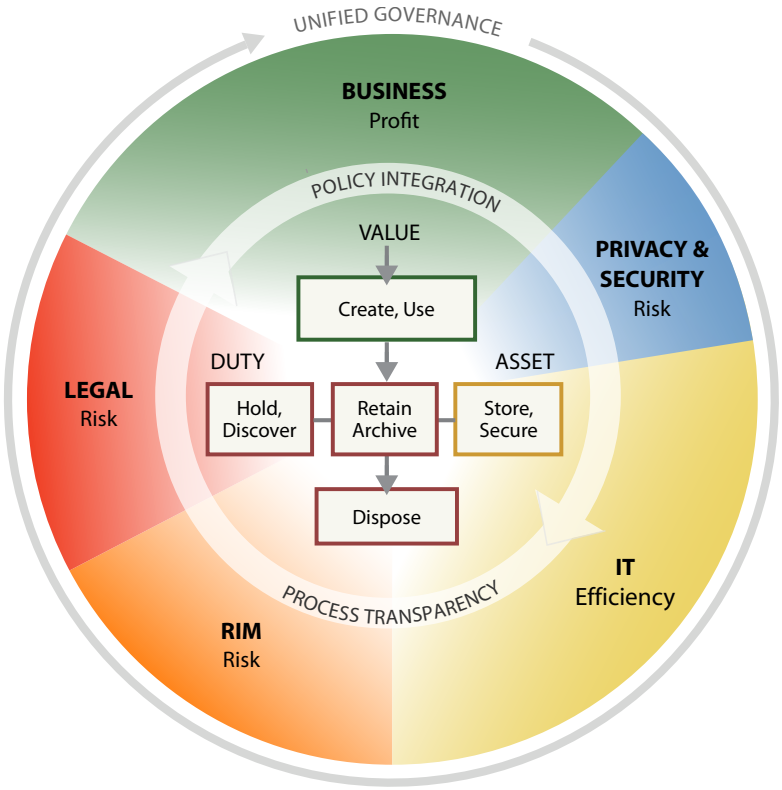
There is a simple strategy that can dramatically change information and ediscovery economics--dispose of unnecessary data. To achieve the strategy, legal, records, business, and IT organizations must work in concert to more precisely and efficiently determine what data stays and what data goes. By connecting historically-siloed groups with proven ILG tools and business processes, organizations can achieve transparency allowing them to determine: What information should be collected and preserved as potential evidence in litigation, what information has ongoing business value and should be retained in the lowest cost manner during its useful lifecycle, and what information is required for regulatory purposes and for how long. The remainder can then be deleted and the infrastructure reclaimed. The goal is to achieve a "steady state" where capacity is continuously applied to new, useful information as aged and fully depreciated data with no remaining utility value is deleted.



Information Governance Reference Model (IGRM)

Unifying disparate and siloed processes and practices in legal, records, business, and IT is the means to achieving cost and risk reduction goals on the path to improved information economics. While these stakeholders have different—and often, conflicting--agendas and responsibilities, no individual stakeholder can be truly effective without working in concert with the others. Historically, these camps have been at odds, debating whether risk mitigation or IT efficiency or business profit trumps the other as an organization's most important objective. This reference model clarifies that all three objectives are important. To achieve them, policy and process transparency along with a unified governance model are required across joint information stakeholders.

The IGRM diagram provides a framework for defining a unified governance approach to information and underscores the importance of linking information duties and value to the data assets under the management of IT. This linkage is critical to ensuring availability of valuable information, reducing risk, and enabling disposal of unnecessary information. The IGRM is a responsibility and logical model rather than a document or case lifecycle (such as EDRM or models from ARMA and AIIM). It helps to identify the stakeholders, define their respective "stake" in information, and highlights their intersection and dependence upon each other. More importantly, it exemplifies the program's goal of effective, efficient governance.



Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Information Governance Reference Model / © 2012 / v3.0 / edrm.net

Navigating to the Desired End State

Once the end state cost and risk reduction goals have been set and the program model and strategy defined, it's time to benchmark the current state of an organization's costs, risks, and processes. From there, organizations need to establish the pace of improvements along with the path to goal achievement.

Excess Cost and Risk

Accurately assess where the organization is today

- Data volume
- IT cost
- eDiscovery costs
- Risk and the current cost of risk mitigation

Processes across legal, records, privacy, business and IT

Means of Achievement

Define the governance framework, operating structure and action

- Organization, responsibilities, and decision making models
- Measurement periods, reporting cadence, and accountability
- Processes involved and improvements required to achieve objectives
- Capacity and capabilities required to operationalize process improvements
- Execution plans by process and workstream responsibilities
- Tools and instrumentation that provide capacity and capability
- Communications and training program
- Audit onset

Value Created by Lower Cost and Risk

Define the specific cost and risk reduction objectives and fiscal milestones for achievement

- IT run rate cost reduction and cost avoidance targets by fiscal period
- eDiscovery cost reduction and avoidance targets by fiscal period
- Risk reduction target by process and pace of achievement (including lowering the cost of mitigation)
- Quarterly and annual financial impact of the program and the process improvement and instrumentation activities that will drive achievement

Setting Quantifiable Cost and Risk Reduction Goals

As a complement to data governance and compliance efforts, an Information Lifecycle Governance program can significantly improve the economics around information management and e-discovery as well as reduce risk. Because an effective program defines policies for when to keep data while instrumenting governance policies across data and infrastructure, it enables companies to realign information management and infrastructure with information value in a comprehensive and systematic way. This alignment and focus on information economics is a tremendous cost reduction lever for the enterprise.

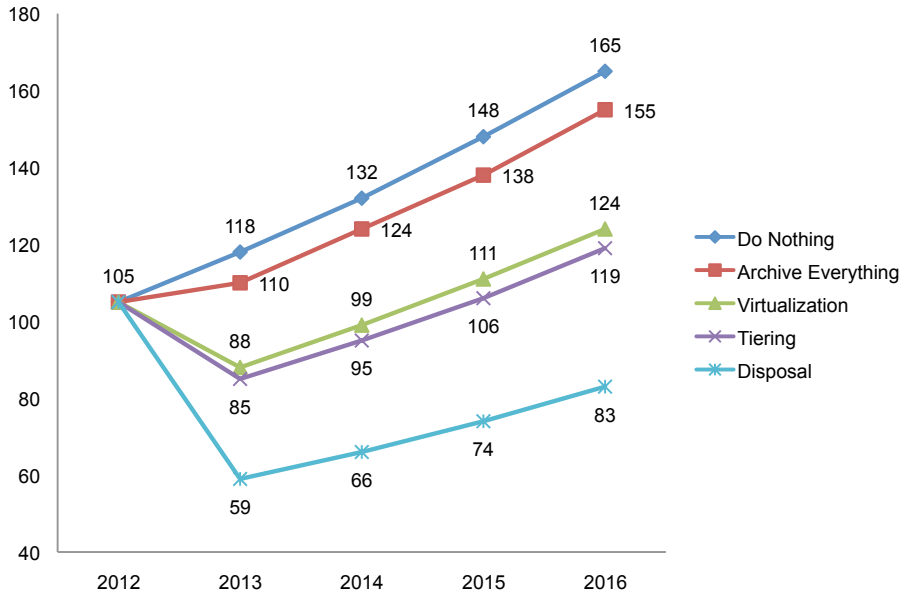
To break through organizational and budget barriers, the program should highlight the value to enterprise stakeholders with primary focus on how to quantify and achieve:

1. Lower storage and infrastructure costs from defensible disposal
2. Lower risk through improved governance instrumentation
3. Lower e-discovery costs through governance instrumentation and lower enterprise data volume

For organizations with rapid volume growth, the only way to contain and control the costs of storage and ediscovery over a five or 10-year horizon may well be disposal of unnecessary data. For any organization considering "big data," this may be true over a much shorter time horizon.

Storage Cost Projection

5PBs at 40% Volume Growth with 20% Unit Cost Growth



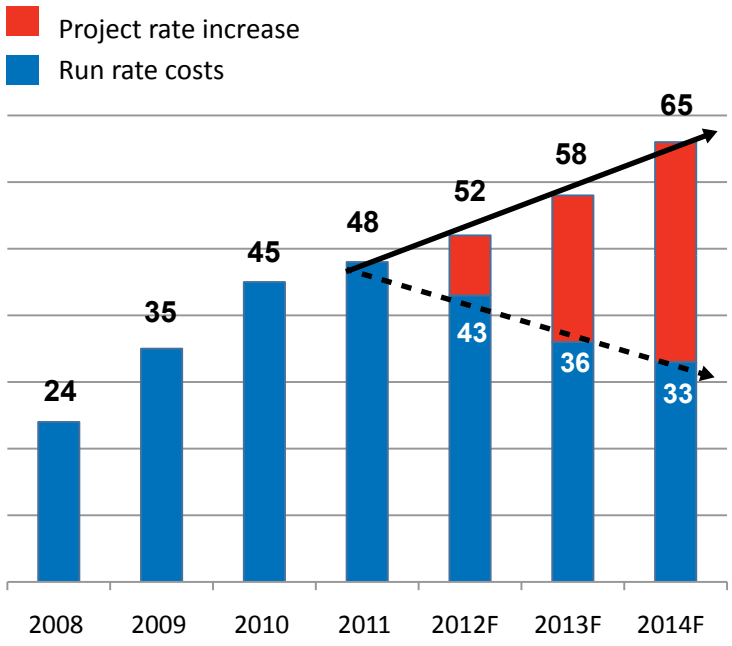
While there are many nuances to an ILG program's primary goals, thorough analysis and framing of these three objectives will create executive relevance for your program. Targeting this particular trio of goals will also galvanize initial action and become the focal point for ongoing measurement of goal achievement.

Storage Cost Reduction

As companies defensibly and consistently dispose of unnecessary information, they find that a significant amount of what was stored was in fact debris, data no longer having value or needed to be retained to meet legal or regulatory requirements. Data debris often accounts for more than half of the total data store as well as the corresponding storage assets. Conversely, companies that don't actively dispose of unnecessary data find themselves facing a compounding cost dynamic that is not sustainable given the dramatic year-over-year escalation of data volumes.

Defensible disposal, therefore, creates a tremendous dividend for IT since almost all IT costs are associated with the amount of data, applications, and hardware in the environment. As retention schedules are aligned with and instrumented onapplications and servers, organizations can rationalize storage allocation with the business need for information along with the duration of that need. Total expenses encompass the direct procurement costs of storage and storage refresh, which are tied proportionately to the total amount of storage required. Other costs related to bandwidth, storage management staff, servers, and software also must scale according to the amount of data stored. Focusing on this direct procurement spend is often the most effective way to communicate the benefits of defensible disposal to the CFO while linking the measureable and defined savings targets to an overall information economics objective.

Storage Costs ($M)

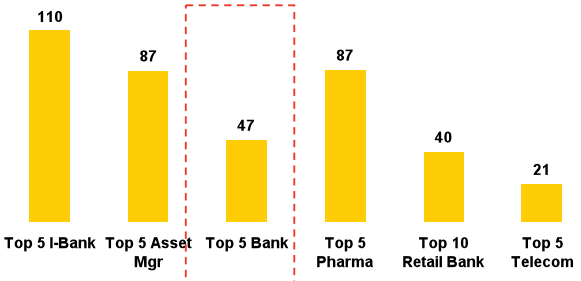


Application Decommissioning Cost Reduction

Providing visibility and instrumentation for retention policies and ediscovery in the data as well as in the information environment enables organizations to more readily decommission applications no longer containing high-utility information along with redundant systems that are no longer tasked with maintaining data. By doing so, companies save on both hardware and software costs by scaling back server and storage consumption, terminating leases and software licenses, and re-using them for other purposes when and where they add value.

Annual cost savings estimates $40K per application is a conservative estimate for industry norms

Cost Savings per Application Estimates Application Decommissioning Projects ($K per App.)



# of Apps	4	3	450	46	20	1140
Annual Cost Savings ($M per Year)	0.5	0.3	21	4	0.8	24

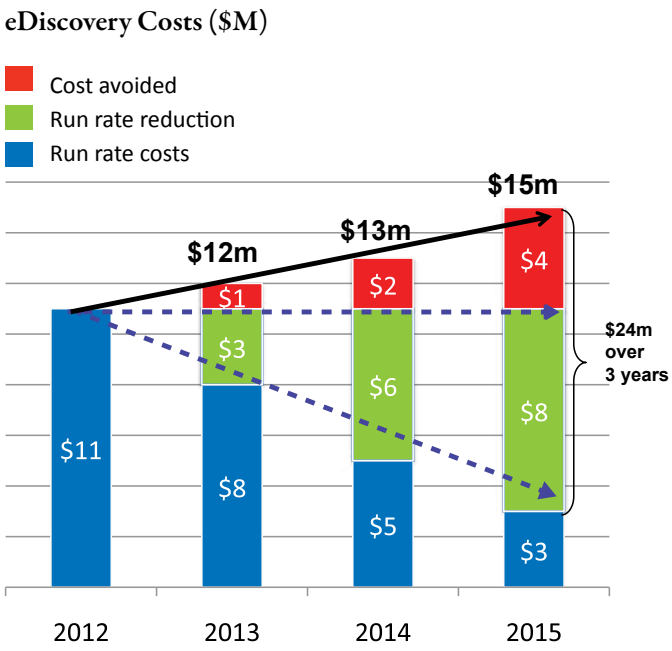
Potential for incremental cost savings

App. Decommissioning Annual Savings per App. ($ K per year)			
COST	**Small App.** (4 cores, 0.5 TB)	**Large App.** (12 cores, 1 TB)	**Avg. App.** (8 cores, 0.75TB)
S/W Costs			
Oracle DB	14	43	$14K
H/W Costs			
Servers	25	75	**$25K**
Storage	0.5	2	**$0.5K**
Total Cost	40	120	$40K
# of Apps	40	100	70
Cost Savings per year ($M)	$1.6M	$12M	$7M

eDiscovery Cost Reduction

Much like IT costs, legal ediscovery costs are also largely a function of data volume. Matter duration and run rate legal fees are influenced by the scope (number of custodians and documents/files to review) of an ediscovery initiative because the optimum settlement point is often when the costs and risks of continuing a dispute outweigh the costs and risks to settle or otherwise resolve. Lack of insight or visibility into true ediscovery costs lead to late settlement decisions and excess run rate costs—neither of which enhance settlement dynamics. (Here it's important to note that 97% of all matters settle before trial, and of the 3% that do go to trial, half of those settle before the trial concludes.) Therefore, improvements to the ediscovery process can increase transparency, enable defensible disposal of unnecessary data, and considerably reduce outside legal fees—all of which are contributing factors to improving information economics.

Volume	Value	Metric
Matters	500	# per year
Active Matters	260	# per year
Collection Volume	66	GB/matter
Collected Volume Increase	10	% per year
Reduction Drivers		
Volume Reduction due to Disposal	20	% GB
Volume Reduction due to Accurate Culling	20	% GB
Matters settle early	5	% matters



Risk Reduction

Expanding data volumes are not only a strain on the IT and storage budgets, they are also overwhelming governance processes and creating operational complexity that in turn, increases compliance and financial risks. Holding on to more data was historically perceived as an effective risk mitigation strategy, but for most organizations, this is no longer the case. By assessing specific information lifecycle governance processes across legal, records, IT, and the business, the risk reduction benefits of the program and the risks of inaction can be communicated internally in a more quantified manner.

ILG Process		Potential Risk of Failure
A	Employees on Legal Holds	Custodians are not identified and potentially relevant information is inadvertently modified or deleted.
B	Data on Legal Hold	Actual, rogue or IT managed data sources missed in hold execution; potentially relevant information is inadvertently modified or deleted.
C	Hold publication	IT or employees migrate, retire, or modify data because they lacked hold visibility.
D	Evidence Collection	Dynamic, diverse information facts not considered in preservation and collection planning, and data is overlooked. No follow through on information identified in custodian interviews. Collection failure from overlooked source, departing employee, incomplete prior collection inventory, communication and tracking errors.
E	Evidence Analysis & Cost Controls	Material issues in dispute are poorly understood until well after strategy established and expenses incurred. Excessive data causes litigation costs to exceed dispute value.
F	Legal Record	Unable to readily assemble, understand, or defend preservation and discovery record. Failures in custodian and data source management. Preservation, collection detected long after occurrence, causing unnecessary remediation cost and risk.
G	Master Retention Schedule & Taxonomy	Company is unable to comply or demonstrate compliance with its regulatory record keeping obligations. Disparate nomenclatures for records make application of retention schedules/procedures difficult to apply and audit.
H	Departmental Information Practices	IT 'saves everything' which increases discoverable mass, complexity, and legal risk; IT disposes of information of business value undermining enterprise operation. Procedures for retention/disposal difficult to articulate and defend and unapplied by line of business.
I	Realize Information Value	Important business decisions are made on missing information or poor quality information, resulting in ineffective decisions. Information is not used shortly after its creation because business has forgotten the source or location of information and can't find it, resulting in cost without corresponding value.
J	Secure Information of value	Information of value is not properly secured against internal security violations or external security breaches; entities can bypass or contravene security policies, practices, or procedures. Failure in securing information deeply heightens privacy issues if information accessed is not properly protected.
K	Privacy & Data Protection	Access, transport, and use limitations are not understood by employees with information custody or collections responsibility, impacting customers' or employees' rights.
L	Data Source Catalog & Stewardship	The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and disposition policies.
M	System Provisioning	Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting, and disposing of information, exposing the company to significantly higher costs and risks.
N	Active Data Management	New, valuable, aging, and useless data are commingled within the data source, its back up, and its non-production instances. Business users waste their time sifting through debris to find what they need without success. IT costs soar. Organization is exposed to privacy, security, and legal risks.
O	Disposal & Decommissioning	IT is unable to dispose of data and decommission systems causing significant and unnecessary costs and risks; IT improperly disposes of data causing unnecessary risk and legal or business expense.
P	Legacy Data Management	IT is unable to associate data with business stakeholders or ensure legal duties are met, leading to oversight in collecting evidence and unnecessary legal and operating costs.
Q	Storage Alignment	Storage is over-allocated, misaligned with business needs, and consumes unnecessary capital; IT is unable to reclaim storage and eliminate cost after data is deleted resulting in unnecessary expenses.
R	Audit	Unable to demonstrate reasonable efforts to establish and follow governance policies and procedures increases sanctions risks, penalties, and judgments while eroding customer trust.

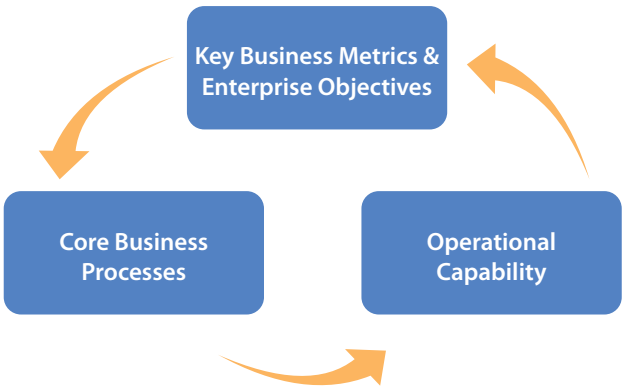
Operationalizing the Strategy

Translating strategy into tactics and turning goals into results requires clear connection between the business objectives, the processes and actions required to achieve them, the capacity to execute those actions, and measurement for accountability.

Business Goals ⇨ Relevant Processes ⇨ Process Capacity ⇨ Metrics Against Goals

Defined business objectives for the program and how achievement will be measured over time

» Cost and risk reduction through value-based information management, rigorous compliance, and defensible disposal



Ensure accountability for outcomes and provide visibility to operational issues that impede results

» Vehicle for management support and issue resolution aligned with clear business goals

Defined business processes and practices required to achieve the business objectives

» 18 specific processes that institutionalize defensible disposal, value-based archiving and retention, and rigorous compliance

Defined staff and instrumentation required to enable core business processes to perform as required to achieve objectives

» People and tools necessary for processes at target operating maturity

Governance Processes Required to Lower Cost and Risk

There are 18 specific business processes across legal, records, privacy, the business, and IT functions that collectively dictate information economics and which must operate at high reliability and high maturity levels to defensibly dispose of unnecessary data and mitigate risk.

ILG Process		Brief Description
A	Employees on Legal Holds	Determining employees with information potentially relevant to an actual or anticipated lawsuit or government investigation
B	Data on Legal Hold	Determining information, records and data sources that are potentially relevant to an actual or anticipated lawsuit or government investigation
C	Hold publication	Communicating, syndicating and executing legal holds to people, systems and data sources for execution and compliance
D	Evidence Collection	Fact finding and inquiry with employees with knowledge of a matter in dispute to determine potentially relevant information and its whereabouts and sources. Collecting potential evidence in response to an agreed-upon request with an adversary or government agency
E	Evidence Analysis & Cost Controls	Assessing information to understand dispute and potential information sources and for determining, controlling and communicating the costs of outside review of relevant information
F	Legal Record	Documenting the custodians and data sources identified, the legal hold and collection activities over multi-year matter lifecycle
G	Master Retention Schedule & Taxonomy	Defining an information classification schema that reflects the organization structure; cataloging, updating, and mapping the laws that apply to each class in the countries in which the organization operates to determine regulatory record keeping obligations; establishing and managing a network of records liaisons to help establish what records may exist where.
H	Departmental Information Practices	Using an enterprise information taxonomy, cataloging which information each business organization values, generates or stores by class, where they store it and how long it has utility to them; results in retention schedules for information and enables data source-specific retention schedules that reflect both business value and regulatory requirements
I	Realize Information Value	Gaining timely access to and ability to apply information in the course of their work, including the ability to harness information of quality as it ages and the ability to use relevant information with or without author context to maximize the enterprise value of information.
J	Secure Information of value	Determining a schema for the various levels of information importance and the corresponding security needed; using an enterprise information taxonomy and network of liaisons across the business, cataloging which information each business organization generates or stores and assigning the appropriate security level; communicating these security needs to employees who generate, use, manage, and store information.
K	Privacy & Data Protection	Assessing privacy duties by data subject and data location, including overlapping obligations for information and information elements and a means of communicating these requirements to those employees who generate, use, access, and store information
L	Data Source Catalog & Stewardship	Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures
M	System Provisioning	Provisioning new servers and applications, including associated storage , with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protecting data elements subject to privacy rights
N	Active Data Management	Differentiating high value actively used data by the business from aging data of value to regulators only or less frequently accessed data; results in increased accessibility, security, privacy; aligns and enables data value with storage tiering by value.
O	Disposal & Decommissioning	Disposing data and fully decommissioning applications at the end of their business utility and after legal duties have elapsed
P	Legacy Data Management	Processes, technology and methodologies by which data is disposed and applications fully decommissioned at the end of their utility and after legal duties have elapsed
Q	Storage Alignment	The process of determining and aligning storage capacity and allocation to information business value and retention requirements, including optimizing utilization targets, storage reclamation and re-allocation after data is deleted to link storage cost to business need for data stored
R	Audit	Testing to assess the effectiveness of other processes, in this instance the processes for determining, communicating, and executing processes and procedures for managing information based on its value and legal duties and disposing of unnecessary data

Strategy Check

Programs and projects often fail in institutionalizing information lifecycle governance to improve information economics because it is a significant undertaking that touches many areas of the organization. Validate that your strategy and tactics address the common causes of failure:

1. Lack of clarity or metrics on the desired business outcomes – no "Point B"
   - » No clear cost reduction and risk reduction goals established so the organization, and management in particular, loses interest in execution
   - » No way to measure progress towards goal or hold people accountable so initial value is never achieved

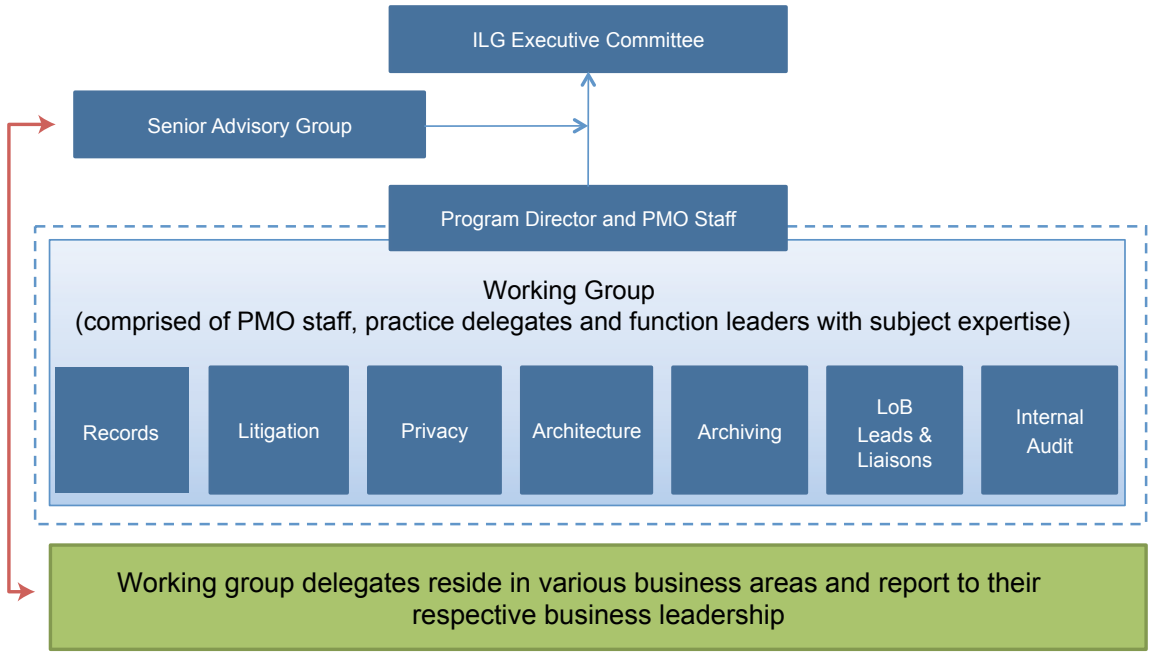
2. 2. Lack of clarity on which processes and levers drive "Point B" cost and risk reduction outcomes
   - » No translation of objectives and outcomes to the work and processes required to achieve them, which undermines results
   - » No plan to address missing processes and levers that are pre-requisites to results or to practical operational achievement impeding the overall effort

3. Lack of capacity and capability to execute or operationalize processes or pull levers required to achieve "Point B" cost and risk reduction outcomes
   - » Lack of capacity to operate required processes at the target maturity level
   - » Lack of capability from insufficient process maturity or failure to instrument processes
   - » Lack of tools to sustain or execute processes or selection of tools that don't function at required level of maturity

Program Leadership

Organization Model

Executive sponsorship and accountability are critical to achieving the cost and risk reduction goals of an ILG program as is leadership that can unify delegated process stakeholders across functional disciplines as well as once-disparate practices. At the highest level, companies should establish an Executive Committee that includes the CIO, CFO, General Counsel, and other officers. A Senior Advisory Group, comprised of line of business leaders (division executives), provides the staff and support necessary for achieving goals and should be routinely kept in the loop on progress and issues. A Program Office, set up to complement these working bodies, should take the lead in driving and measuring progress toward goals, and in turn, direct the efforts of a Working Group responsible for maturing and instrumenting the relevant processes.



Achievement Measurement and Accountability

Consistent measurement and reporting is perhaps the most critical success factor. The program cost and risk reduction goals along with the timeline for achieving those goals form the basis for executive dashboards, management reports, and accountability. Align the timing of reporting and content to fiscal periods, set clear financial goals, and compare them to both prior period measurements as well as initial defined targets.

Avoid the pitfall of measuring performance without also measuring the capacity to perform. All too often, goals are set (most likely by management) without the operational wherewithal to achieve the intended results. Capacity planning and monitoring are critical because resource issues and allocations can undermine results—especially for cross-functional projects. The composition of the Executive Committee and Senior Advisory Group, combined with the reporting cadence, are a primary means of anticipating and addressing these issues.

Operational capacity is measured for each of the 18 processes and considers maturity level (process capability) and the people and/or tooling required to perform or operate the process at the target maturity (process capacity). The combination of both measures is a key indicator to how the processes will perform over time while also serving as a leading indicator of where companies will fall short in achieving cost or risk reductions.

Achievement Measurement & Accountability

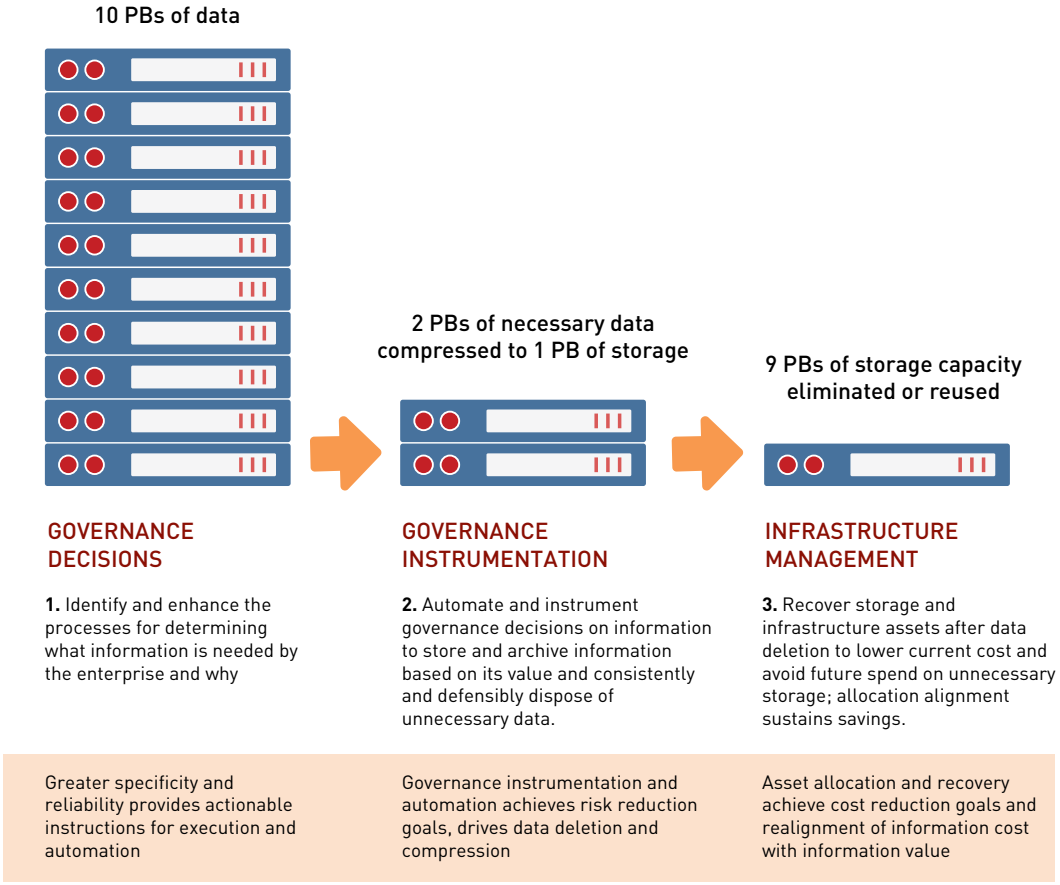
Because an information lifecycle governance program results in material financial savings, the Executive Committee and senior advisors will be motivated to encourage progress and hold their organizations accountable for outcomes. Frequent, consistent measurement against established goals ensures appropriate progress while helping to identify and remove obstacles that might get in the way of short- and long-term outcomes.

	Executive Committee	Senior Advisory Group	PMO Leader	Working Group Delegates	
Quarterly Business Review	✓	✓	✓	✓	Cost, risk and capacity status by period and against established targets *until goals are achieved*. Issues unresolved in monthly operations dialogue.
Monthly Operations Status		✓	✓	✓	Summary progress reporting on workstreams. Issues unresolved at PMO level.
Bi-Weekly Project and Workstream Status			✓	✓	Detailed project and workstream status reporting including deliverable status, action items, and issues requiring resolution.
Exception Reporting	✓	✓	✓	✓	Issues and road blocks that may impede achievement of expected cost and risk reduction targets and/or the timing of their achievement.

Once lifecycle governance is institutionalized and instrumented, Internal Audit provides after-the-fact reporting on process failures, can help identify root causes of failure, and can ensure organizational accountability for remedying process, instrumentation, or monitoring issues (discussed in the next section). Audit criteria, one of the more essential processes, should be designed into the program as a core part of an ILG strategy.

From Policy to Savings

Because an information lifecycle governance program results in material financial savings, the Executive Committee and senior advisors will be motivated to encourage progress and hold their organizations accountable for outcomes. Frequent, consistent measurement against established goals ensures appropriate progress while helping to identify and remove obstacles that might get in the way of short- and long-term outcomes.

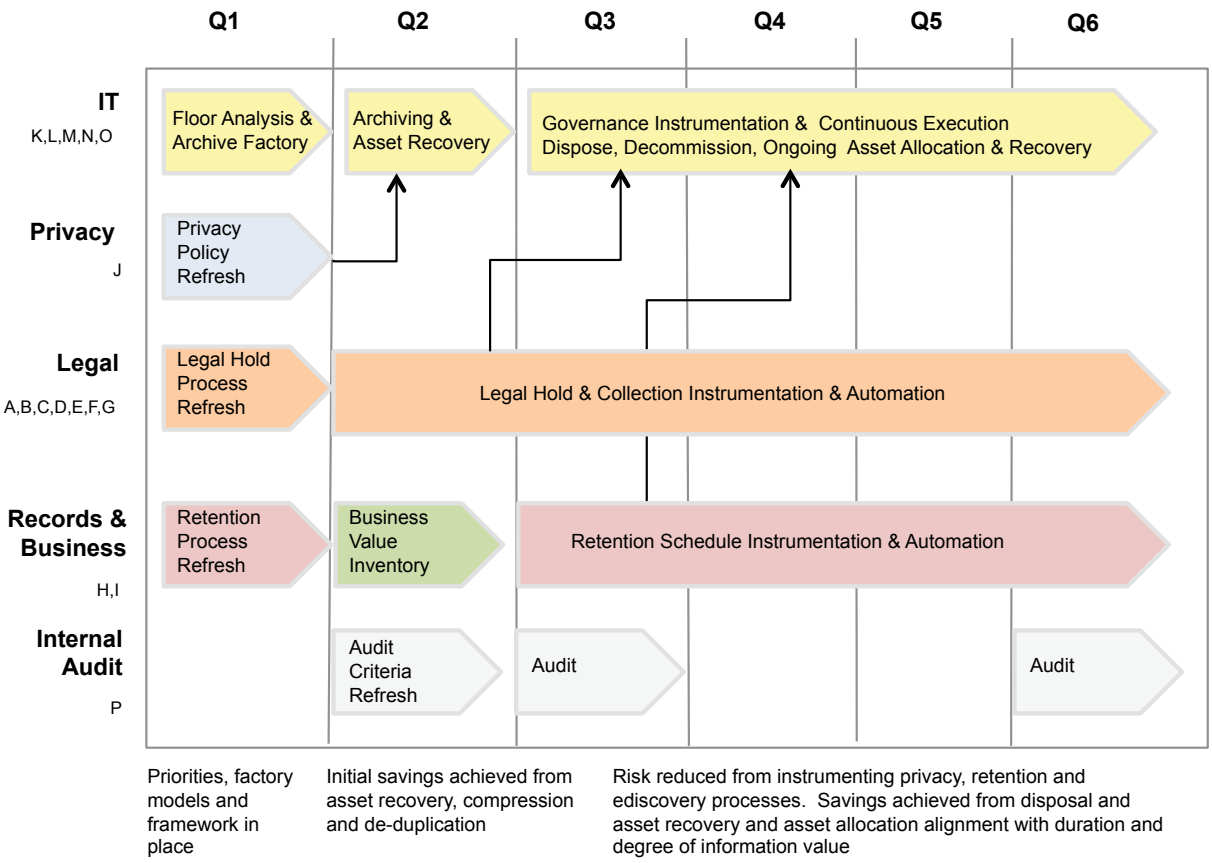


There are three competencies that must co-exist to maximize cost and risk reduction benefits:

1. Governance policy management to foster precise decisions on what data is needed and what is available, while making it actionable for both the people and the systems requiring the data
2. Governance instrumentation and policy execution in the data environment to ensure that data is stored, tiered, managed, accessible, and deleted based on its specific utility to the organization
3. Asset allocation and recovery to optimize the deployment of storage and infrastructure commensurate with data value, eliminate or recover infrastructure as data is deleted, and continuously align infrastructure costs with information utility

Execution Timeline

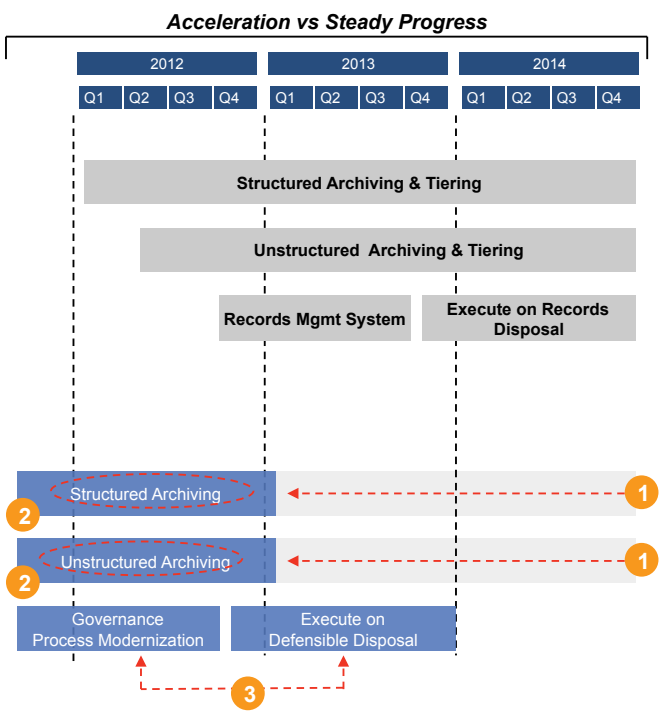
Achieving cost and risk reduction goals requires parallel efforts and multiple-threaded workstreams directed by the PMO. In addition to analyzing the data environment and establishing an archive and tiering factory, organizations need to make improvements to legal hold, records and retention, and privacy processes to enable defensible disposal and complete governance instrumentation and automation for sustained savings.

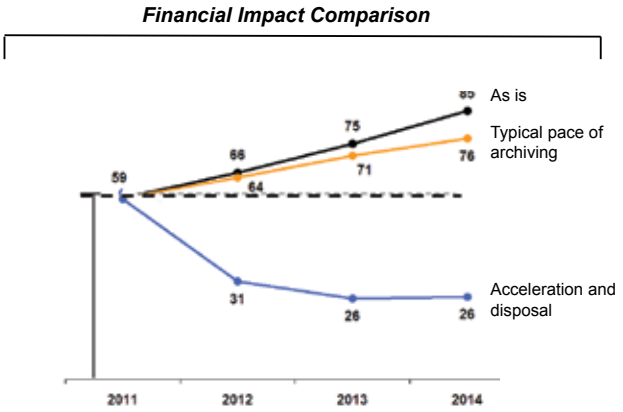


Time is one of the most potent levers for lowering cost because storage costs recur and grow annually. By rapidly decreasing the amount of data stored, companies can not only save money faster, but also save more money over time.

3 Savings Levers

1. **Accelerate time to and total value** by compressing the program from 3 to 2 years
2. **Expand the scope** of data addressed by the program to achieve faster, greater run rate **reduction**
3. **Defensibly dispose of unnecessary information by** managing data by its value

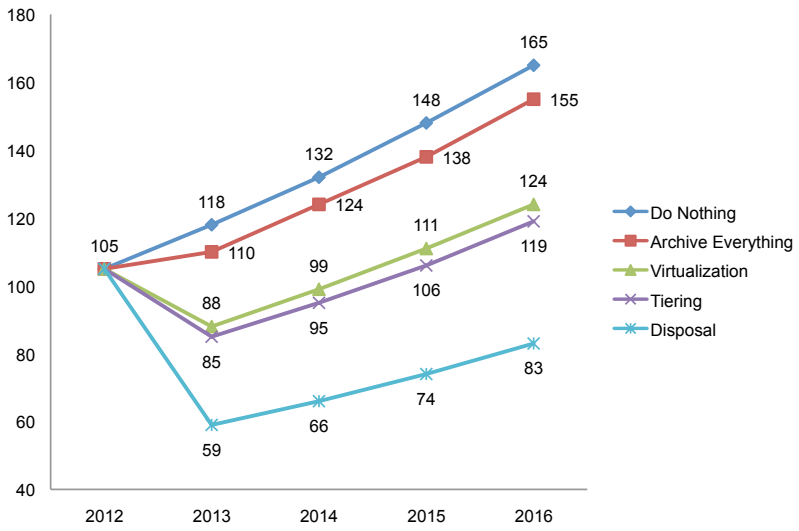




Because data volume compounds year over year, slower-paced programs or those that aggressively, but not defensibly, dispose of unnecessary data will likely fail to achieve cost reduction goals or sustain cost reduction over a long-term period. Based on the data volume, costs, and growth assumptions shown in the chart below, disposal produces $139 million in savings over a five-year period with significant run rate reduction immediately and sustainably lower run rate costs (continuous savings) over time.

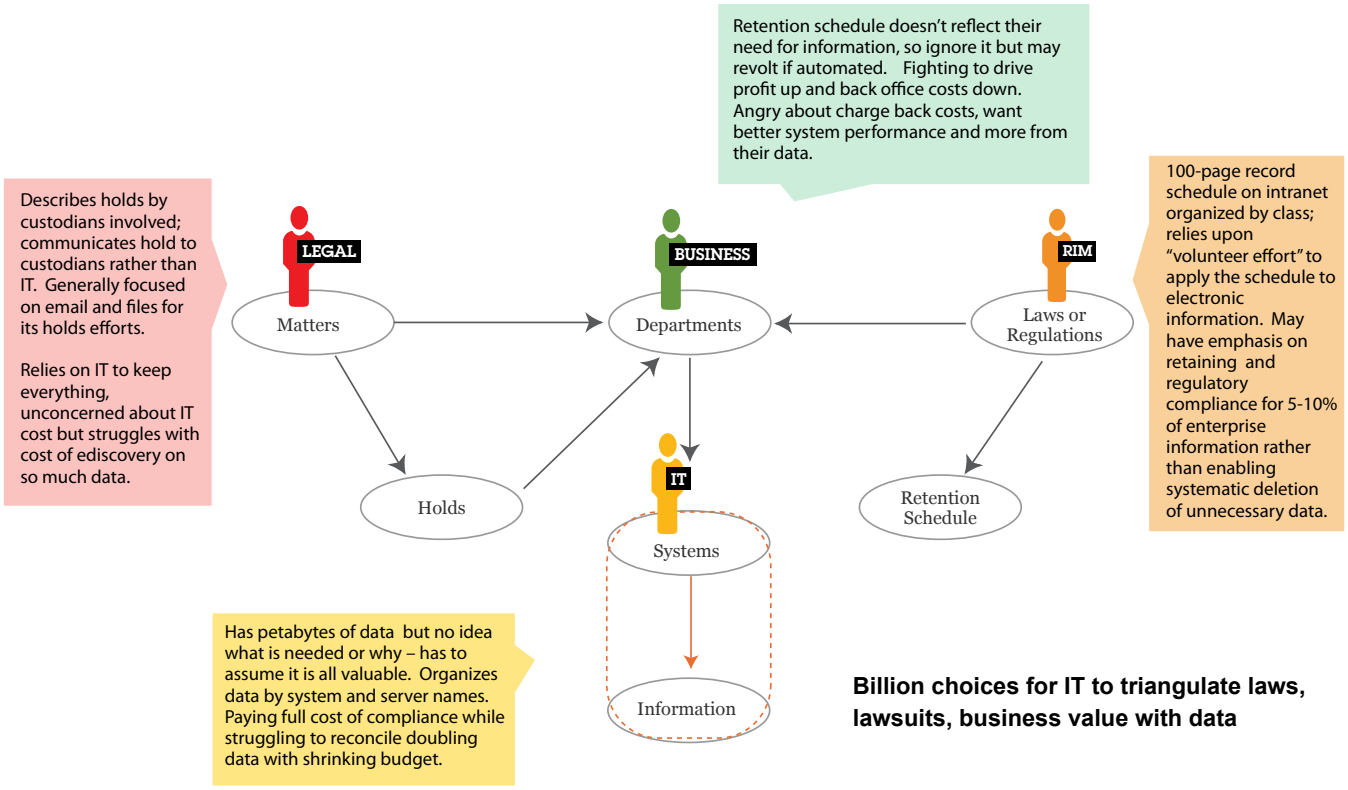
Storage Cost Projection

5PB's at 40% with 20% Unit Cost Growth



Process Maturity and Management

For most organizations, the root cause of excess data and the cost and risk it creates is the inability to consistently and systematically associate information value and obligations with information assets. This is difficult in practice because the form and scope of legal holds and retention schedules don't readily align with the form in which information is managed, the volume and growth of it, and the operational dynamics this creates for IT organizations. While policies and requirements may be formally published, they are often not instrumented on data itself – as data volume doubles and IT budgets contract, policy is very difficult to execute consistently.

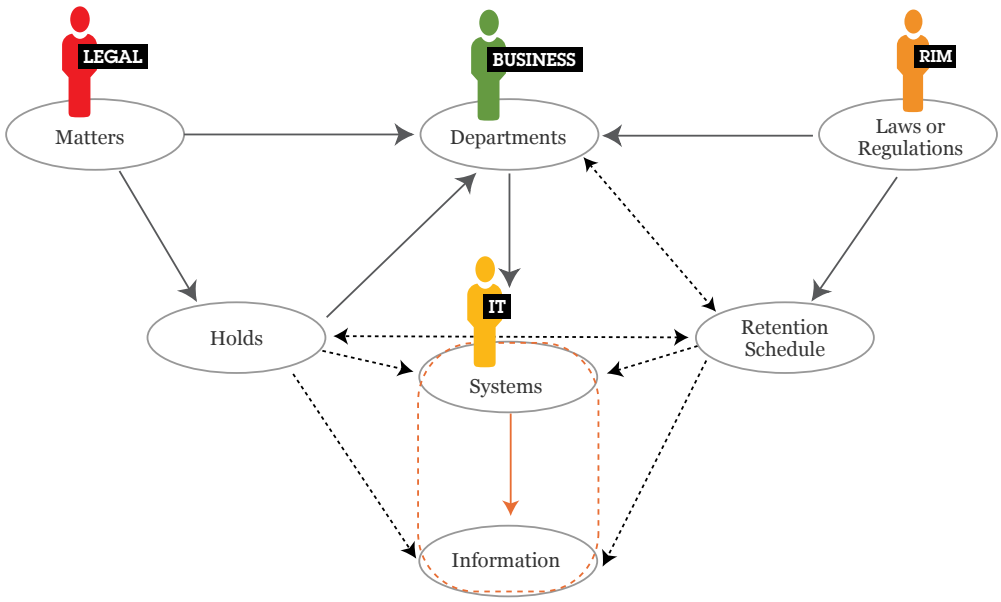


To achieve the cost and risk reduction benefits of an ILG program, legal hold and retention practices must be extended and enhanced so they are automated to serve the vast majority of enterprise information. Systematically applying retention and disposition to structured data often drives substantial savings, particularly when done in concert with tiering and archiving practices to further compress the remaining data of value. Legal and records staff are often surprised to learn that messaging and files may comprise a relatively small portion of total storage and data assets. Therefore, considering the costs associated with data should be a critical factor when setting priorities for process improvements and governance instrumentation.

IT needs accurate schedules that can be automated across the petabytes of data under management in order to realize capacity and cost savings. The result is a shift in focus from retention schedules designed for physical records to broadly-applied schedules that can be reliably instrumented on the data itself.

Privacy policy must also be instrumented to effectively execute retention schedules. At the same time, improvements in the way systems are provisioned and decommissioned and how assets are allocated and recovered are also necessary. Creating a data source catalog that is shared across policy makers in legal, records, the business, and compliance and establishing an organization charged with its execution is a backbone process for information lifecycle governance, which can also function as a key lever for improving information economics.

The PMO and Working Group should assess process maturity and establish the timeline for process improvements designed to meet the target operational maturity in alignment with cost and risk reduction goals. Key to their responsibilities: Enhancing the scope and form of legal holds and retention schedules so they can be consistently and automatically applied to data, incorporating business value more holistically, and instrumenting the linkage of holds and schedule to information assets closing any remaining operational gaps.



LEGAL

Modernize eDiscovery Process

- ✓ Precise, reliable legal holds
- ✓ Assess evidence in place, collect less
- ✓ **Lower legal risk, cost**

IT

Optimize Information Volume

- ✓ Dispose and retire unnecessary data
- ✓ Optimize storage based on value
- ✓ **Lower information cost**

BUSINESS

State Information Value

- ✓ Guidance on information utility
- ✓ Participate in volume reduction
- ✓ **Align around value**

RECORDS

Modernize Retention Process

- ✓ Address electronic information
- ✓ Executable schedules can be automated
- ✓ **Lower legal risk, cost**

PROCESS	
A	Employees on Legal Holds
B	Data on Legal Hold
C	Hold publication
D	Evidence Collection
E	Evidence Analysis & Cost Controls
F	Legal Record
G	Master Retention Schedule & Taxonomy
H	Departmental Information Practices
I	Realize Information Value
J	Secure Information of Value
K	Privacy & Data Protection
L	Data Source Catalog & Stewardship
M	System Provisioning
N	Active Data Management
O	Disposal & Decommissioning
P	Legacy Data Management
Q	Storage Alignment
R	Audit

Processes Capability and Maturity

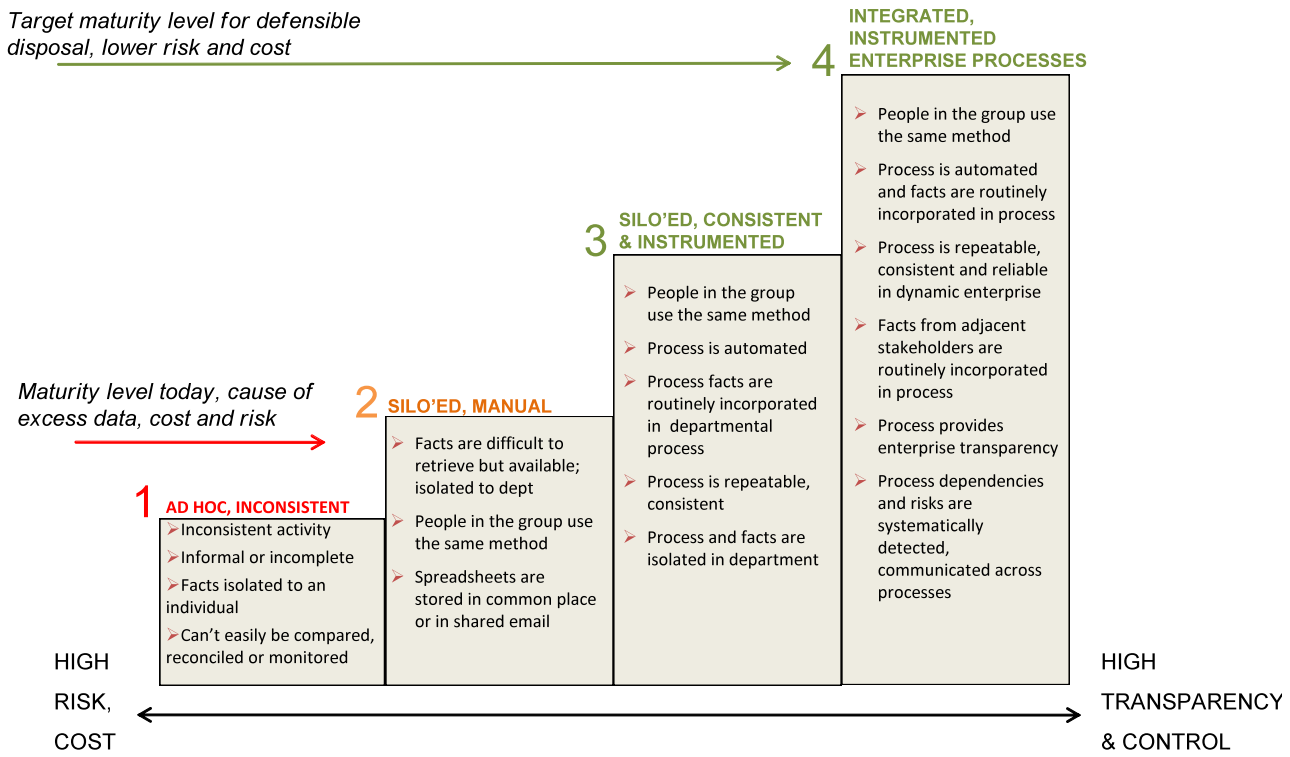
Having a clear understanding of the process maturity levels along with the organization's current process capabilities and practices will help frame the ILG work effort and change management required to improve information economics and achieve defensible disposal. The 18 core processes for improving information economics take into account the way an organization defines demand (what information is needed, why, and for how long) and how it manages supply (what is provisioned, managed, decommissioned, and disposed).

Level 1 is an ad hoc, manual, and unstructured process performed differently by each practitioner; only the individual practitioner has access to the process facts or results. These processes are highly unreliable and difficult to audit.

Level 2 is a manual process with some consistency in how it is performed across practitioners within a particular function or department; only the department has access to the process facts and results, and often these are embedded in multiple spreadsheets and seldom accessed. These processes can be more reliable, but still very difficult to audit.

Level 3 is a semi-automated process performed consistently within a department with process facts and results readily accessible to departmental stakeholders. Cross-departmental stakeholders who participate in or are dependent upon the process are not integrated. These intradepartmental processes are more consistent and can readily be audited; however audit results may reflect their lack of interdepartmental collaboration.

Level 4 is an automated and cross-functional process that is performed consistently with inclusion of dependent stakeholders across multiple departments. Process facts and results are readily available across organizations. These processes have the lowest risk, highest reliability, and are readily and successfully audited.



Business Processes Critical to ILG

	Process		Brief Description	Process Risk or Immaturity Consequences	Level 1: Ad Hoc, Manual, Unstructured
	A	**Employees on Legal Holds**	Determining employees with information potentially relevant to an actual or anticipated lawsuit or government investigation.	Custodians are not identified and potentially relevant information is inadvertently modified or deleted.	Multiple custodian spreadsheets managed by the individual paralegal or attorney.
	B	**Data on Legal Hold**	Determining information, records and data sources that are potentially relevant to an actual or anticipated lawsuit or government investigation.	Actual, rogue or IT managed data sources missed in hold execution, potentially relevant information is inadvertently modified or deleted.	Limited collection from data sources, custodian rather than information based; spreadsheet tracking/lists.
	C	**Hold publication**	Communicating, syndicating and executing legal holds to people, systems and data sources for execution and compliance.	IT or employees migrate, retire or modify data because they lacked hold visibility.	Manual notices, confirmations, no escalations Description of information hold requires interpretation and manual effort to comply.
LEGA	D	**Evidence Collection**	Fact finding and inquiry with employees with knowledge of a matter in dispute to determine potentially relevant information and its whereabouts and sources. Collecting potential evidence in response to an agreed-upon request with an adversary or government agency.	Dynamic, diverse information facts not considered in preservation and collection planning, data is overlooked; no follow through on information identified in custodian interviews. Collection failure from overlooked source, departing employee, incomplete prior collection inventory, communication and tracking errors.	Duplicate spreadsheets of custodians and information in IT and Legal; multiple copies of collected data.
	E	**Evidence Analysis & Cost Controls**	Assessing information to understand dispute and potential information sources and for determining, controlling and communicating the costs of outside review of relevant information.	Material issues in dispute are poorly understood until after strategy established and expenses incurred. Excessive data causes litigation costs to exceed dispute value.	Over-collect from custodians, over scope custodians. No culling of clearly irrelevant information before sending to vendor or outside counsel. Don't assess costs prior to collection and review; no cost baseline available.
	F	**Legal Record**	Documenting the custodians and data sources identified, the legal hold and collection activities over multi-year matter lifecycle.	Unable to readily assemble, understand or defend preservation and discovery record. Failures in custodian and data source management. Preservation, collection detected long after occurrence and cause unnecessary remediation cost and risk.	Each attorney tracks their own matters, status.

Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions	Your Level
Custodian lists are kept in Word or Excel in a shared location or in a shared mailbox. Questionnaire mailed to custodians, responses compiled manually for collection / counsel follow up.	Systematic scope and selection by organization, people from current and historical organization data. Systematically track all custodians in all holds including multiple holds per custodian. Scope terminated/ transferred employees involved. Interviews are systematically done, responses compiled and responses are automatically flagged and escalated as appropriate.	Real-time update of custodian roles, transitions, responsibilities, automatic employee transition/transition alerts by attorney and matter; copy or cross reference custodian lists across similar matters. Scope is revisited and refined at least quarterly to release or include custodians. Individual responses to interview questions are propagated to hold scope and interview results shared with outside counsel to interview by exception. Level 3 capabilities.	
Identify data sources by organization; understand back up procedures. Questionnaire mailed to custodians, responses compiled manually for collection /counsel follow up.	Have linked legacy tapes and data sources to organizations and open holds/collections.	Automatically scope people, systems, production and back up data, information and records in holds; scope terminated employee data and legacy data/tapes where applicable. Scope is revisited and refined at least quarterly to release or include data. Can scope directly from a data source catalog shared with business liaisons, IT, Info Sec, and other data quality stakeholders with reliability. IT interviews are done both periodically and in matter context and responses are aggregated for individual matters and across the legal team.	
Centralize reply email box for confirmations, Process well communicated, all holds on intranet.	Systematically send notices and reminders, require and track confirmations, ability to manage exceptions, employees can look up their holds at any time. Communications tailored to recipient role (IT, RIM, employee).	Publish to system, propagate hold, automate hold enforcement. IT Staff have continuous visibility to current discovery duties, holds during routine data management activities; automatically flag records in appropriate systems. Holds are timely released and release syndication is done with same rigor as hold syndication. Level 3 capabilities.	
Centralized, version controlled spreadsheets of custodians and information; evidence server organized by matter folder but no inventory by custodian and data.	System log of collection requests by matter, issuer and collector. Collection logging is done by discovery staff in a shared system. An inventory of evidence is well managed and not overlooked in scoping other matters. Interview results and insights are used to inform the collection activity.	Interview results are automatically incorporated into custodian or data source specific collection instructions without rekeying. IT or collection staff can efficiently and automatically collect by custodian and content without re-logging the request or recollecting the same data. Collection data and chain of custody is automatically logged. IT and legal share complete transparency on collections and legal can monitor progress and process while IT can process work by custodian or data source efficiently. From their browsers, legal staff can collect directly from custodians and systems with precision. Evidence is not duplicated in multiple locations and it is timely disposed. Level 3 capabilities.	
High quantity of data for review. Some basic processes for culling of irrelevant information by basic means such as date ranges used in some cases. Estimate costs on the "big matters" in spreadsheets or by outside counsel.	Quantity of data reviewed from tightly scoped custodians, leveraging prior scoping histories. Consistent & enforced culling performed by preferred vendors utilizing objective criteria such as keywords, date ranges, file types, domain names & data sources. Discovery cost forecasts available as the hold is scoped, costs are calculated continuously.	Consistently limit scope of collection and review; early case assessment performed before collection for earliest/optimized matter resolution, advanced culling techniques employed leveraging visual analytics; defined & repeatable process for providing outside counsel early case assessment before processing, manage cost at portfolio level. Level 3 capabilities.	
Formal, but manual reporting of open holds; no summary reporting on interviews, collections, response.	Automated reminders and escalations, online audit trail, management reporting on discovery status, visibility within legal department across custodians, collected inventory, and matters.	Appropriate visibility across IT, Legal and Business; self-service dashboards for legal obligations, tasks, risk and cost reduction opportunities. Level 3 capabilities.	

	Process		Brief Description	Process Risk or Immaturity Consequences	Level 1: Ad Hoc, Manual, Unstructured
RIM	G	**Master Retention Schedule & Taxonomy**	Defining an information classification schema that reflects the organization structure; cataloging, updating, and mapping the laws that apply to each class in the countries in which the organization operates to determine regulatory record keeping obligations; establishing and managing a network of records liaisons to help establish what records may exist where. Potential separate process for **Records Management:** Managing physical and electronic records including their identification, retention, and timely disposition.	Company is unable to comply or demonstrate compliance with its regulatory record keeping obligations. Disparate nomenclatures for records make application of retention schedules/procedures difficult to apply and audit.	Define retention periods only for physical records. Rely on aggregations of similar laws and longest retention period to determine record keeping requirements.
BUSINESS	H	**Departmental Information Practices**	Using an enterprise information taxonomy, cataloging which information each business organization values, generates or stores by class, where they store it and how long it has utility to them; results in retention schedules for information and enables data source-specific retention schedules that reflect both business value and regulatory requirements	IT 'saves everything' which increases discoverable mass, complexity and legal risk; IT disposes of information of business value undermining enterprise operation. Procedures for retention/disposal difficult to articulate and defend and unapplied by LoB.	Departmental information management needs and habits for electronic and physical information are not visible to records management, IT or legal stakeholders (who have no knowledge of actual procedures, information, location, use, or value).
	I	**Realize Information Value**	Gaining timely access to and ability to apply information in the course of their work, including the ability to harness information of quality as it ages and the ability to use relevant information with or without author context to maximize the enterprise value of information.	Important business decisions are made on missing information or poor quality information, resulting in poor decisions. Information is not used shortly after its creation because business has forgotten the source or location of information or can't find it, resulting in cost without corresponding value.	Information is difficult to retrieve or search. After creator loses initial context, it is forgotten and no value is realized. Staff must mine, open and view files on their individual drives to find what they need and access to relevant information they didn't create is exchanged via email.
PRIVACY	J	**Secure Information of Value**	Determining a schema for the various levels of information importance and the corresponding security needed; using an enterprise information taxonomy and network of liaisons across the business, cataloging which information each business organization generates or stores and assigning the appropriate security level; communicating these security needs to employees who generate, use, manage, and store information.	Information of value is not properly secured against internal security violations or external security breaches; entities can bypass or contravene security policies, practices, or procedures. Failure in securing information deeply heightens privacy issues if information accessed is not properly protected.	Has no policy for protecting valuable info and high would be has policy, maps security required to data source capabilities and enforces on data.
	K	**Privacy & Data Protection**	Assessing privacy duties by data subject and data location, including overlapping obligations for information and information elements and a means of communicating these requirements to those employees who generate, use, access, and store information.	Access, transport and use limitations are not understood by employees with information custody or collections responsibility and customers or employees rights are impacted.	Each country and business keeps a list of applicable privacy rules. Implementation is done locally and informally.

Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions	Your Level
Retention schedule updated to reflect physical and electronic records. Country schedules share a common taxonomy.	Established retention period for regulated information and information important from a policy perspective. The specific or actual laws that dictate retention periods are known and on clearly mapped to each record class so law changes can be easily traced and decisions readily defended on law. Electronic and physical records are sequestered and are both retained and disposed against the schedule.	Retention schedules reflect regulatory, policy and business value and encompass all information enabling them to be executed on records repositories, application and archived data, and physical records; legal holds can be applied by record class and suspend automated disposal. There is a shared library of country protocols for ediscovery, privacy, and retention to form a comprehensive view. Schedules align with and are systematically used to dispose of production and back up data whether structured, unstructured, electronic, physical, record or business information. Level 3 capabilities.	
Inventories of departmental information management practices and source information are used to develop retentions schedules and coordinate physical records (via a network of records coordinators focused on physical records management).	Departmental liaisons work with their line of business to identify information of value, its duration of value and where it is managed; this informs more comprehensive retention schedules for all information (regulated, unregulated, electronic, physical). Business is able to request changes to master schedule and department/country schedules at the rate of business change.	Retention schedules are automatically executed across the information environment. Cost and benefit are weighed in determining retention periods and the enterprise impact is considered. Schedule changes are syndicated to IT and directly to systems for execution of both retention and disposition. When business objectives or laws change, schedules are updated and stakeholders notified. Legal and IT have transparency to what information each line of business has where and for how long to inform ediscovery and data management. Level 3 capabilities.	
Information for a group is organized in shared drives and collaboration sites. Employees must search multiple drives and collaboration sources to find what they need; relevant information is extracted by opening multiple files, emails, documents, or reports; structured and unstructured data must be harvested separately and manually correlated.	Application data and business process data can be searched by departmental staff in the course of their work from within the system.	Search and analytics enable employees to realize value and to apply information to decision making in real time even as context erodes across information sources and types; assertions on value and sources of information made in processes H and I are used to ensure availability and accessibility of information the business defined as valuable. The cost of information to the enterprise is consistent and appropriate over its lifecycle.	
Each business unit defines their own information categories and assigns security level and attributes. Individual employees are responsible for understanding and applying security levels manually.	A common information taxonomy or categories are used across business units as basis for determining security levels and value attributes; this information is maintained in source or system accessible to information security staff. Some data is classified systematically.	Uses a common enterprise information taxonomy with processes H and I, shares liaison network and cataloging efforts, and results in a single view of applicable value and regulatory requirements for stakeholders by business area and information category. Enables security owners and systems owners to identify gaps between security required and data source capabilities to reduce exposure. Information is properly classified automatically and secured appropriately for its value. Execution of retention, privacy and security requirements can be efficiently executed without redundancy or conflicts.	
Privacy and data protection requirements are tracked in the privacy office and corporate policies are published on the intranet; implementation decisions are left to local business and system owners.	There is an accurate catalog of privacy laws and policies by country accessible to privacy. Policy communications are routine and semi-automated to records, business and system stakeholders. Critical systems are provisioned with some privacy controls.	Systems are provisioned with access, masking, and controls to protect privacy; information stakeholders in business, legal and IT have access to privacy constraints in real time; litigation has access to current privacy law and protocol and factors law into evidence collection/analysis plan; process is audited. Level 3 capabilities.	

	Process		Brief Description	Process Risk or Immaturity Consequences	Level 1: Ad Hoc, Manual, Unstructured
IT	L	**Data Source Catalog & Stewardship**	Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures.	The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and disposition policy.	No common definition of data sources and data elements exists across IT, legal, business and records. No linkage of asset to the specific applicable business value or legal duties.
	M	**System Provisioning**	Provisioning new servers and applications, including associated storage , with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protecting data elements subject to privacy rights.	Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting and disposing of information, exposing the company to significantly higher costs and risks.	Retention, preservation, collection and/or disposition are not considered prior to provisioning.
	N	**Active Data Management**	Differentiating high value actively used data by the business from aging data of value to regulators only or less frequently accessed data; results in increased accessibility, security, privacy; aligns and enables data value with storage tiering by value.	New, valuable, aging, and useless data are commingled within the data source, its back up and its non-production instances. Business users waste their time sifting through debris to find what they need without success. IT costs soar. Organization is exposed to privacy, security and legal risks.	Data is managed over time as the system was provisioned and new, valuable, aging, and useless data are co-mingled within the data source, its back up and its non-production instances.
	O	**Disposal & Decommissioning**	Disposing data and fully decommissioning applications at the end of their business utility and after legal duties have elapsed.	IT is unable to dispose of data and decommission systems causing significant unnecessary cost and risk; IT improperly disposes of data causing unnecessary risk and legal or business expense.	IT 'keeps everything' because it has no systematic way to determine obligations or value.

Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions	Your Level
IT has an asset tracking system. IT does not have visibility to holds or retention schedules for any given asset.	IT maintains an asset database for its use; IT manually enters legal holds, business liaison and retention rules for each asset/system. Legal maintains its own data map for ediscovery purposes.	Shared data source catalog across IT, legal, records and business stakeholders which is used to express information assets and relevant business needs and legal obligations. Catalog as source of truth for provisioning and back up retention/disposition requirements and all back up, archiving and provisioning procedures and decisions are transparent in the catalog. Common definitions are used to describe duties, needs, stewards, employees, laws and lawsuits across ILM&G stakeholders.	
Some systems are manually configured with capabilities to retain and collect, but policy and capability to dispose or preserve are lacking.	Some systems are configured to retain, dispose, preserve and collect data but schedules and instructions are manually applied and configured. Instructions from legal, records and the business on duties and values are communicated in disparate tools and techniques and must be reconciled within IT.	Systems are provisioned with protocol and technical capability to retain/dispose and hold/collect, including a properly authorized retention schedule and business value inventory. Systems are provisioned with the capability to archive data to lower cost storage at the earliest point in time, archive procedures are well defined and archives execute retention/ disposition of approved schedules. Back up is used for disaster recovery only and does not function as long-term archive. Retention schedules, legal holds and collection requests are systematically propagated from their respective initiators; data source catalog is updated to reflect the provisioning, archiving and back up mechanisms.	
End user employees perform hygiene and clean up actions on file shares and systems to ensure function and access. IT performs basic back up and availability functions.	Some archiving is performed to batch off aging data and provide business users with faster access to more frequently used data. Archive approach varies by data source and business unit. Policies for retention, privacy and security are manually applied, if at all.	Data of high value actively used by the business is differentiated from aging data of value to regulators only or less frequently accessed data. Business users have ready access to high value data and spend no time sifting through debris to find it. Data is secured and retained based on its business value. Aging data with declining value is archived or moved to lower cost locations over time; unnecessary data is routinely disposed. Private data is masked based on policy. Back up data complies with the retention schedule and is not used as long-term archive alternative.	
Some systems are manually configured with capabilities to retain, hold, collect or dispose of data. Changes in legal requirements must be manually configured.	IT de-duplicates files and disposes of log files under its control. IT responds to business requests to decommission applications and works with legal on a manual review process to determine if any open legal matters may apply before decommissioning.	Data is automatically deleted at the end of its retention period when no legal hold has been specified; back up data is routinely and systematically overwritten. IT routinely analyzes the data source catalog to identify systems with low business value to proactively determine savings opportunities; IT can easily determine duplicative systems from the business value and taxonomy map for instance consolidation. IT performs routine disposal with transparent, reliable facts on preservation and retention obligations; looks up any asset or employee to determine value, current legal requirements.	

	Process		Brief Description	Process Risk or Immaturity Consequences	Level 1: Ad Hoc, Manual, Unstructured
	P	**Legacy Data Management**	Processes, technology and methodologies by which data is disposed and applications fully decommissioned at the end of their utility and after legal duties have elapsed.	IT is unable to associate data with business stakeholders or ensure legal duties are met, leading to oversight in collecting evidence and unnecessary legal and operating costs.	No hold release notification, no lookup ability.
	Q	**Storage Alignment**	The process of determining and aligning storage capacity and allocation to information business value and retention requirements, including optimizing utilization targets, storage reclamation and re-allocation after data is deleted to link storage cost to business need for data stored.	Storage is over-allocated, misaligned with business needs and consumes unnecessary capital; IT is unable to reclaim storage and eliminate cost after data is deleted causing unnecessary cost.	No reliable means of determining storage requirements and inability to allocate/reclaim based on retention needs. Each DBA determines capacity and capacity is not revisited.
	R	**Audit**	Testing to assess the effectiveness of other processes, in this instance the processes for determining, communicating, and executing processes and procedures for managing information based on its value and legal duties and disposing of unnecessary data.	Unable to demonstrate reasonable efforts to establish and follow governance policies and procedures increases sanctions risks, penalties and judgments and erodes customer trust.	Do not audit retention, holds, disposal processes.

Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions	Your Level
eMail hold release communication from Legal to IT.	IT initiates a process with legal to "reverse engineers" legacy data holds to dispose of unstructured data or back up data.	Legacy data on disk and tape is dispositioned using legal hold inventory enriched with custodian and data sets subject to hold, data subject to ongoing regulatory or legal requirement is isolated and "surrounding" data is disposed; no additional legacy data is accumulated.	
Intensive manual effort to achieve an accurate picture of storage capacity and cost; difficulty assessing and reconciling need, allocation and utilization. Charge backs are used but not reflective of cost facts or cost accounting.	Automated storage utilization reporting and charge back mechanism and transparency to refresh cycles across the inventory. Charge back reporting by tier and organization is reliable and fact based.	Storage is provisioned for new systems commensurate with retention schedules and archive protocols; refresh accounts for capacity availability from continuous deletion and decommissioning activity. Storage cost is weighed in retention schedule approval process and archive decision making; unit cost is available in data source catalog. Current and forecasted storage capacity and costs are transparent and align to business value and data retention schedules. Optimization practice captures benefit of deletion and decomm to avoid continuous capacity addition. Accurate charge back reporting by business unit and source and gap analysis to retention schedule, business value and information cost to inform business decision making on the costs/benefits of storing data over time.	
Verifies that the global retention schedule is published and visible to IT and LOB.	Audits publication of records, privacy, disaster recovery, application lifecycle, and legal hold policies. Does not test execution of the policy.	Establishes and conducts testing procedures for records management, business value inventories, data sources, privacy requirements and legal holds such that information assets are properly defined and retained until their value expires and it is timely disposed when there is no longer a business need or legal duty. Sample tests of organizations and record class for retention and timely disposition. Establishes and conducts testing procedures for legal matters to ensure preservation duties are properly communicated and executed and holds are timely released. Tests data source catalog, back up data, and system provisioning to ensure ability to comply and actual policy adherence. Audits storage provisioning and procurement against retention/disposition/decom schedules.	

Capacity Planning: Map Required Effort to Outcomes

Part of the role of the PMO and Working Group is to establish workstreams along with a roadmap on how to mature and instrument processes. The pace of these efforts must tie to the pace of cost and risk reductions defined in the business goals and program financials.

As a part of the process maturity and improvement effort, responsibilities for each process owner should be defined to reflect the level of maturity, integrity, and reliability required to achieve the cost and risk reduction goals. Each workstream will likely include policy revisions, process and practice improvements, and technology to sustain better practices and ensure transparency and integration across stakeholder processes.

To support the business objectives of the ILG Program, the Legal organization will:

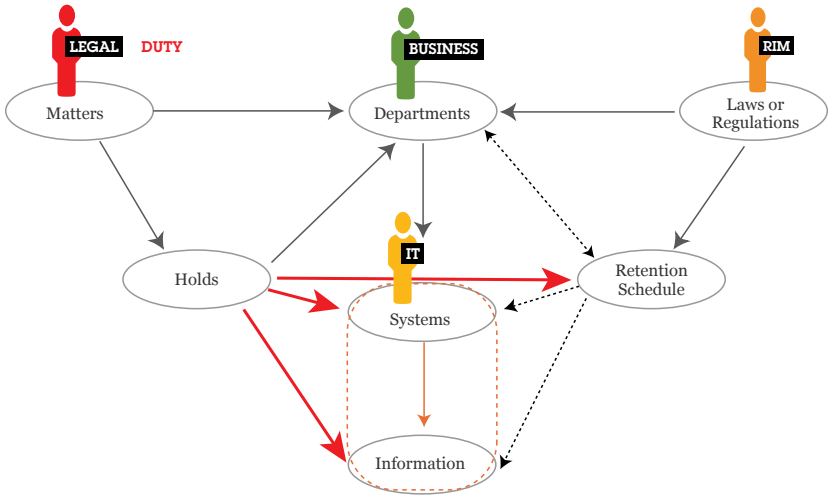
- Maintain an accurate inventory of legal obligations for information by case and scope of obligation, including individuals involved, information scope (dates, terms, elements), and relevant records. The inventory should indicate whether the duties have been satisfied fully or partially as well as how they have been satisfied.
- Precisely define and clearly communicate specific requirements to preserve potential evidence to IT, records, and business stakeholders in a timely manner for each matter, including the individual employees, records, and ranges of data that must be preserved as potential evidence.
- Provide real-time, continuous transparency to current legal obligations for information that can be readily understood and acted upon by stakeholders in IT, records, and business units.
- Affirmatively communicate to and receive confirmation of compliance from employees or records managers; IT staff is relied upon to preserve information in its custody.
- Timely notification to IT, records, and business stakeholders when evidence for a particular matter no longer needs to be preserved.
- Ensure the defensibility of its process through complete, accurate, timely record keeping and closed-loop communications with custodians, IT, and records staff.
- Enable defensible disposal of information through precise, consistent, and timely communication of obligations to individuals, IT, and records staff when the duty arises and as it changes over the course of a matter.
- Work with Internal Audit to assess enterprise preservation procedures.

Capabilities for Legal to Define Holds by People, Records, and Data Involved to Hold, Collect & Produce More Effectively & Efficiently

LEGAL

Modernize eDiscovery Process

- ✓ Precise, reliable legal holds
- ✓ Assess evidence in place, collect less
- ✓ **Lower legal risk, cost**



To support the business objectives of the ILG Program, the RIM organization will:

- Author and distribute a records management policy and provide training materials to employees or contribute content to corporate ethics training program.
- Provide an information taxonomy that can be reliably used across business, IT, and legal stakeholders to define and characterize business information and information required for regulatory obligations.
- Maintain an inventory of regulatory requirements for records updated annually while identifying which laws apply to which classes of information by country or jurisdiction and business area.
- Provide actionable retention schedules that can be routinely and automatically applied by IT and business stakeholders on electronic information to ensure proper record keeping, safe guarding information of value to the business, and timely disposal of information without value or regulatory duty.
- Maintain a network of records liaisons across the business to coordinate and communicate policy, taxonomy, and schedule needs and changes; provide management visibility on liaison status.
- Safeguard information of value to the business. Perform consistent, documented, and precise collection and disposal of electronic and physical records regardless of their form in accordance with the schedule.
- Ensure timely response to regulatory inquiries; enable Internal Audit to test records and retention procedures on physical and digital records.

To support the business objectives of the ILG Program, the IT organization will:

- Retain and preserve information based on its value to the business and legal obligations according to procedures/instructions provided by legal, RIM and business, including aligning technique and technology to value.
- Timely disposal of unnecessary information to lower information costs and related risks.
- Author and follow back-up and disaster recovery policies that limit the retention of back up media to the shortest necessary period to effectively recover from a disaster or failure.
- Maintain an inventory of systems with current business value retention, record requirements, and legal hold obligations for data contained in said systems or stores while ensuring that staff involved in provisioning and decommissioning have access to this inventory in the course of their work.
- Establish and provide a common data dictionary for the organization covering data source, employee, information classification, system classification, law, and lawsuit; it should be accessible for use by legal, records, business, and IT as part of the governance program execution.
- Provision new systems, servers, and storage with automated or manual processes for imposing retention, preservation, and disposition of information in the ordinary course of operation (revise SLDC policies, procedures).
- Align systems and stores with information value, including security, privacy, confidentiality, regulatory, business, and litigation requirements.
- Develop protocols for disposal of data and protocols for storage and disposal of customer data and personally identifiable Information (PII) in concert with information security and privacy stakeholders.
- Enable Internal Audit to test retention/disposition, preservation/collection, and privacy procedures.

RECORDS

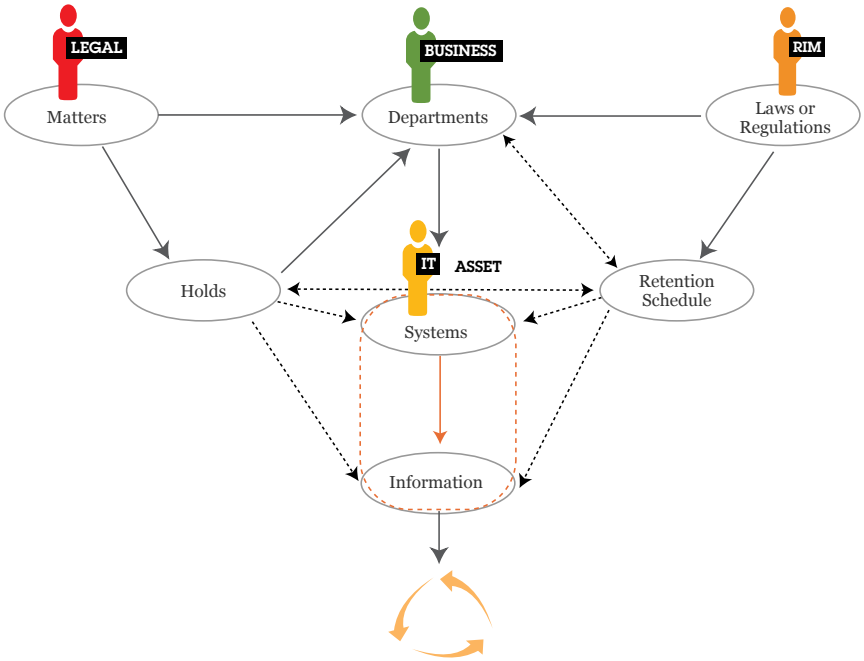
Modernize Retention Process

- ✓ Address electronic information
- ✓ Executable schedules can be automated
- ✓ **Lower legal risk, cost**

IT

Optimize Information Volume

- ✓ Dispose and retire unnecessary data
- ✓ Optimize storage based on value
- ✓ **Lower information cost**



BUSINESS

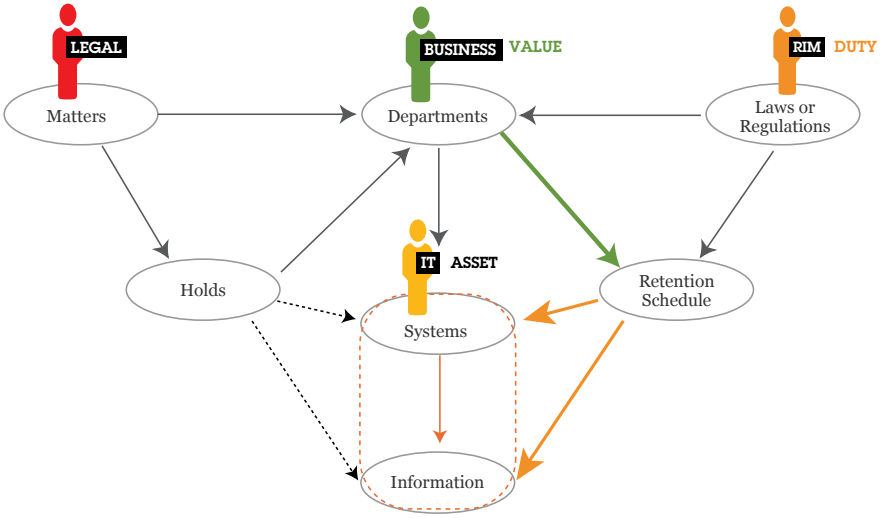
To support the business objectives of the ILG Program, Line of Business organizations will:

- » Ensure a business liaison for governance is able to participate in the program and its processes.
- » Using online tools and a taxonomy provided, participate in a bi-annual value inventory to articulate what information is generated by business teams or departments and the duration of its value to enable IT, records, and legal stakeholders to manage accordingly.
- » Work in concert with IT to optimize the archiving and storage of information based on its utility and management costs in the interest of shareholders regardless of chargeback procedures.
- » As business processes and practices change, proactively initiate changes to the taxonomy, records, and value procedures to reflect business practices and needs.
- » Enable timely disposal of information without value and active participation in the governance program via business leader transparency and accountability for the total unit cost of information (its storage, management, and ediscovery).
- » Participate in Internal Audit on business value inventory procedures.

BUSINESS

State Information Value

- ✓ Guidance on information utility
- ✓ Participate in volume reduction
- ✓ **Align around value**



To support the business objectives of the ILG Program, the Privacy organization will:

- Establish a catalog of privacy laws and policies that is accessible to litigation, records, and IT staff.
- Align with RIM to associate privacy requirements during retention of records and business information.
- Coordinate with litigation in advance of data preservation and collection to ensure that appropriate measures are used for data subjects and jurisdictions.
- Provide education and training to litigation, records, IT, and line of business staff on current and emerging privacy obligations in the United States and rest of world on a periodic basis.
- Enable Internal Audit to effectively test privacy procedures.

To support the business objectives of the ILG Program, the Internal Audit organization will:

- Establish and conduct testing procedures for records management to assess the proper retention and disposition of physical and electronic records to ensure timely regulatory response, defensible disposition, and minimize company risk.
- Establish and conduct testing procedures for business value inventories to ensure that information assets are properly defined and retained until their value expires.
- Establish and conduct testing procedures for legal matters to ensure preservation duties are properly communicated and executed and legal holds are released in a timely manner to reduce company risk.
- Establish and conduct testing procedures for data sources to ensure that information is retained while it has business value or is subject to a legal or regulatory obligation. Also ensures that privacy requirements are met during its retention, and that information is disposed of in a timely fashion when there is no longer a business need or legal duty based on established processes for communicating information duty and value.
- Work with executive management and practice leaders to determine audit readiness and onset.
- Work with the executive committee to do summary reporting on audit findings and with practice leaders on remediation plans.

Audit Processes to Embed Improvements into Ongoing Operations

Internal Audit is an important lever in institutionalizing better governance processes to ensure sustained enterprise benefits from an ILG program. Ongoing internal audit of the 18 processes helps validate that:

- Disposal is and continues to be defensible and on-going
- Compliance with regulatory and legal obligations is achieved
- Assumptions cease to drive decisions on what data must be kept for how long
- Improved processes have been embedded in the operation and continue to function as intended for sustained risk and cost reduction
- Failures in one process that will affect the performance of the other 17 at some juncture are identified and remedied in a timely manner

Audit reporting is critical to management and management should:

- Hold IT, legal, records, and business leaders accountable for audit findings and failures at least annually
- Give both under- and over-retention equal attention as both pose risks to shareholder value

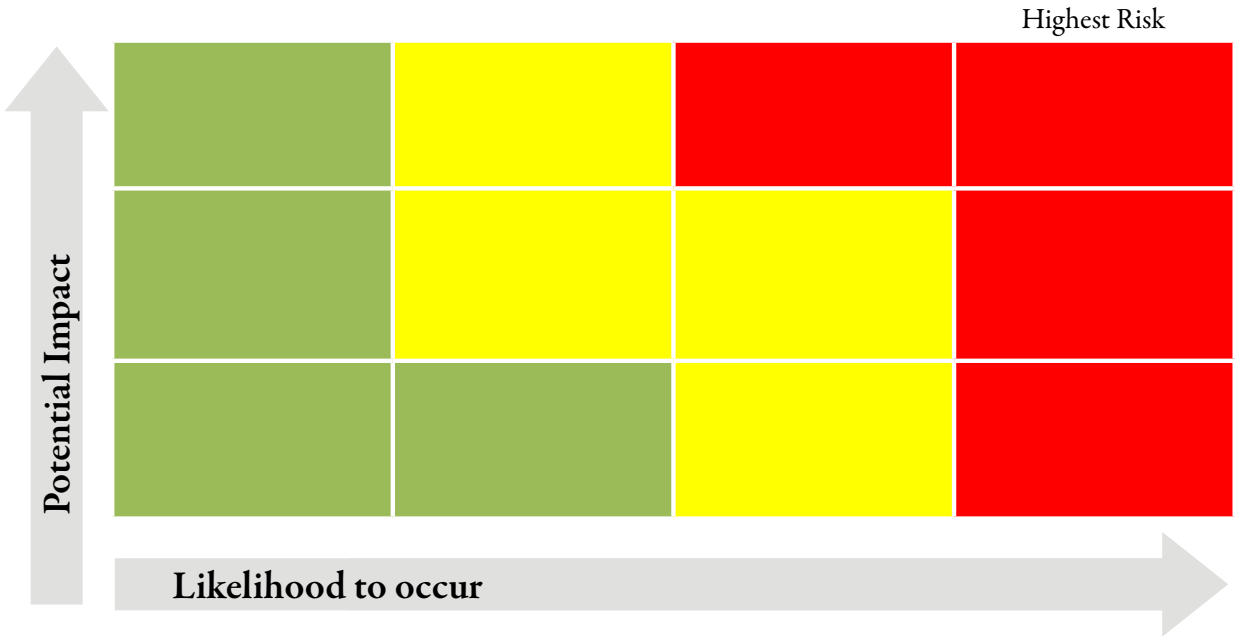
Design audit criteria in tandem with process maturity and improvement levels and before instrumenting governance. The test criteria should exercise the levers for achieving the cost and risk reduction objectives specifically so audits are useful to both the functional leaders and to management. Any lifecycle governance program should focus test criteria on defensible disposal and decommissioning of data as these are the primary savings drivers. Very often, this requires a complete change in the audit program, since most have been focused on retention, but not disposal when retention is no longer required.

Records Compliance Sample testing of organizations and record class for retention, hold placement, and prompt disposition. Example: 6 organizations, 2 records classes each, 100 records per class sampled from first year and last year of retention period. Interval: twice annually Conducted by: internal audit Exception handling: 21 days to respond with remediation plan, 90 days to remediate	**Holds Compliance** Sample testing of matter pool for notice issuance, hold execution, affirmative compliance by employees, records and IT, and hold release at matter disposition Example: 25 matters and all custodians and sources Interval: quarterly Conducted by: internal audit Exception handling: Immediate notice to corporate counsel, 2 days to respond and remediate
Business Value Catalog Sample by organization and data source for currency and accuracy of business value inventory, value statements, and sources/stores identified Example: 6 organizations, all information classes Interval: twice annually Conducted by: records management and LOB leader Exception handling: 21 days to respond with remediation plan, 90 days to remediate	**Data Management** Sample testing by data source for currency of business value inventory, hold placement, retention schedule execution and disposal, back up and DR methods and media, and security protocols Example: 10 sources Interval: twice annually Conducted by: internal audit Exception handling: 21 days to respond with remediation plan, 90 days to remediate for over-retention; 2 days to respond and remediate and immediate notice to corporate counsel for under retention or legal hold failure

Information lifecycle governance uniquely requires processes across the different functions to perform consistently well to lower costs and risk. A single functional stakeholder slippping back to siloed processes and practices or falling short in achieving the necessary level of maturity and transparency can undermine all processes and goal achievement for the overall ILG program. Audit is an excellent mechanism to ensure that function owners are held accountable for their enterprise impact.

Risk Heat Map

1. Using the 18 processes and their risks, consider your facts.
2. Plot the current process risks on the graph by placing the letter for each process on the grid where it belongs.
3. Plot the risk level if your organization had level 3 and level 4 capabilities



PROCESS	
A	Employees on Legal Holds
B	Data on Legal Hold
C	Hold publication
D	Evidence Collection
E	Evidence Analysis & Cost Controls
F	Legal Record
G	Master Retention Schedule & Taxonomy
H	Departmental Information Practices
I	Realize Information Value
J	Secure Information of Value
K	Privacy & Data Protection
L	Data Source Catalog & Stewardship
M	System Provisioning
N	Active Data Management
O	Disposal & Decommissioning
P	Legacy Data Management
Q	Storage Alignment
R	Audit

High risk requires constant monitoring and review, immediate escalation on failure or impending failure. 50% likelihood

Moderate risk requires frequent monitoring to prevent and detect; costly to correct or mitigate. Between 10% -50% likelihood

Low risk does not require constant monitoring and is easy to prevent, detect, correct, defend. Less than 10% likelihood

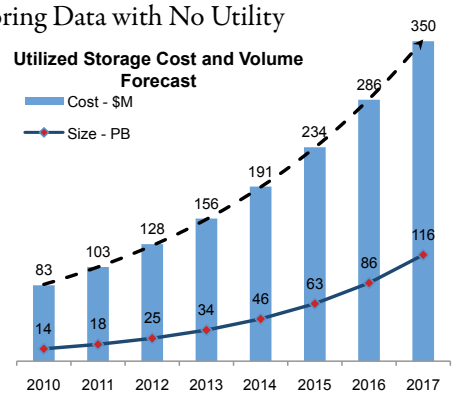
Cost Levers

Process Drivers

Scorecard

1 Storage Infrastructure:

Storing Data with No Utility

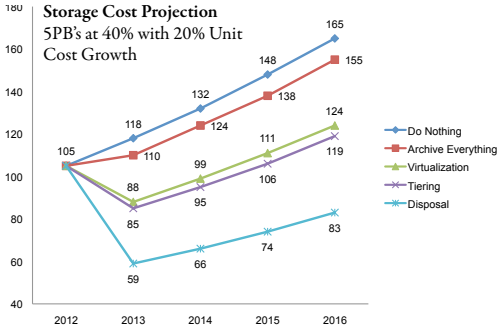


Excess storage cost (processes N and Q) resulting from over-accumulation and/or inability to delete data for lack of certainty on legal holds, regulatory requirements or business value. Costs correlate to capabilities in process A) scoping people on hold, B) scoping data on hold, C) publishing holds, G) master retention schedule, and H) departmental information practices.

	1	2	3	4
N				
Q				
A				
B				
C				
G				
H				

2 Storage Infrastructure:

Storing Data at Cost Higher than Value

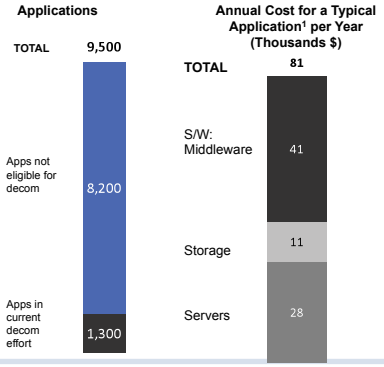


Excess storage and infrastructure cost resulting from managing and storing data on storage tiers and price points in excess of information value, particularly aging data, non-production instances, and back ups. Costs correlates to capabilities in process H) master retention schedule, I) departmental information practices, M) system provisioning, and Q) storage alignment.

	1	2	3	4
H				
I				
M				
Q				

3 Applications:

Instances without Business Value

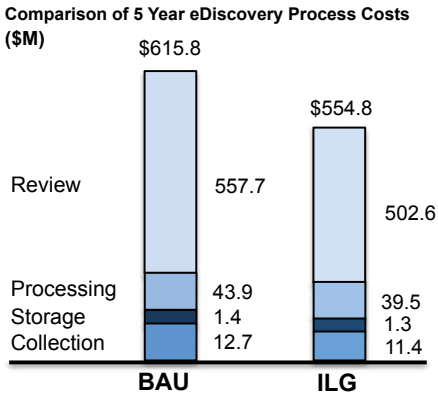


Delayed or partial application decommissioning (process M and O) from inability to discern which data is required by legal, regulators and business. Cycle time delays lead to excess run rate. Costs correlates to capabilities in process A) scoping people on hold, B) scoping data on hold, C) publishing holds, G) master retention schedule, and H) departmental information practices.

	1	2	3	4
M				
O				
A				
B				
C				
G				
H				

4 eDiscovery:

Costs of Collection and Review



Excess ediscovery and outside counsel fees from over collection of data from lack of visibility to what data exists, inability to collect with precision, excess data across the information environment, and late case resolution with excess run rate legal costs or excessive ediscovery cost relative to case merits. Costs correlates to capabilities in process L) data source catalog, N) active data management, O) disposal, P) legacy data management, H) departmental information practices, G) master retention schedule as well as D) evidence collection and E) evidence analysis and cost controls.

	1	2	3	4
L				
N				
O				
P				
G				
H				
D				
E				

Level 1: Facts known only to individual practitioner
Level 2: Facts accessible with difficulty by others within same practice

	ILG Process		Brief Description
	A	Employees on Legal Holds	Determining employees with information potentially relevant to an actual or anticipated lawsuit or government investigation
	B	Data on Legal Hold	Determining information, records and data sources that are potentially relevant to an actual or anticipated lawsuit or government investigation
	C	Hold publication	Communicating, syndicating and executing legal holds to people, systems and data sources for execution and compliance
	D	Evidence Collection	Fact finding and inquiry with employees with knowledge of a matter in dispute to determine potentially relevant information and its whereabouts and sources. Collecting potential evidence in response to an agreed-upon request with an adversary or government agency
	E	Evidence Analysis & Cost Controls	Assessing information to understand dispute and potential information sources and for determining, controlling and communicating the costs of outside review of relevant information
	F	Legal Record	Documenting the custodians and data sources identified, the legal hold and collection activities over multi-year matter lifecycle
	G	Master Retention Schedule & Taxonomy	Defining an information classification schema that reflects the organization structure; cataloging, updating, and mapping the laws that apply to each class in the countries in which the organization operates to determine regulatory record keeping obligations; establishing and managing a network of records liaisons to help establish what records may exist where.
	H	Departmental Information Practices	Using an enterprise information taxonomy, cataloging which information each business organization values, generates or stores by class, where they store it and how long it has utility to them; results in retention schedules for information and enables data source-specific retention schedules that reflect both business value and regulatory requirements
	I	Realize Information Value	Gaining timely access to and ability to apply information in the course of their work, including the ability to harness information of quality as it ages and the ability to use relevant information with or without author context to maximize the enterprise value of information.
	J	Secure Information of value	Determining a schema for the various levels of information importance and the corresponding security needed; using an enterprise information taxonomy and network of liaisons across the business, cataloging which information each business organization generates or stores and assigning the appropriate security level; communicating these security needs to employees who generate, use, manage, and store information.
	K	Privacy & Data Protection	Assessing privacy duties by data subject and data location, including overlapping obligations for information and information elements and a means of communicating these requirements to those employees who generate, use, access, and store information
	L	Data Source Catalog & Stewardship	Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures
	M	System Provisioning	Provisioning new servers and applications, including associated storage , with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protecting data elements subject to privacy rights
	N	Active Data Management	Differentiating high value actively used data by the business from aging data of value to regulators only or less frequently accessed data; results in increased accessibility, security, privacy; aligns and enables data value with storage tiering by value.
	O	Disposal & Decommissioning	Disposing data and fully decommissioning applications at the end of their business utility and after legal duties have elapsed
	P	Legacy Data Management	Processes, technology and methodologies by which data is disposed and applications fully decommissioned at the end of their utility and after legal duties have elapsed
	Q	Storage Alignment	The process of determining and aligning storage capacity and allocation to information business value and retention requirements, including optimizing utilization targets, storage reclamation and re-allocation after data is deleted to link storage cost to business need for data stored
	R	Audit	Testing to assess the effectiveness of other processes, in this instance the processes for determining, communicating, and executing processes and procedures for managing information based on its value and legal duties and disposing of un-necessary data

Level 3: Facts readily available and frequently used in departmental actions and decisions
Level 4: Facts readily available and fully integrated across related enterprise processes, used by all stakeholders in decision and action.

Risk		
Low	Mod	High

Maturity Scale				Potential Risk of Failure	Potential Impact	Likelihood to Occur
1	2	3	4	Custodians are not identified and potentially relevant information is inadvertently modified or deleted		
				Actual, rogue or IT managed data sources missed in hold execution, potentially relevant information is inadvertently modified or deleted		
				IT or employees migrate, retire or modify data because they lacked hold visibility		
				Dynamic, diverse Information facts not considered in preservation and collection planning, data is overlooked; no follow through on information identified in custodian interviews. Collection failure from overlooked source, departing employee, incomplete prior collection inventory, communication and tracking errors		
				Material issues in dispute are poorly understood until after strategy established and expenses incurred. Excessive data causes litigation costs to exceed dispute value		
				Unable to readily assemble, understand or defend preservation and discovery record. Failures in custodian and data source management. Preservation, collection detected long after occurrence and cause unnecessary remediation cost and risk		
				Company is unable to comply or demonstrate compliance with its regulatory record keeping obligations. Disparate nomenclatures for records make application of retention schedules/procedures difficult to apply and audit		
				IT 'saves everything' which increases discoverable mass, complexity and legal risk; IT disposes of information of business value undermining enterprise operation. Procedures for retention/disposal difficult to articulate and defend and unapplied by LoB		
				Important business decisions are made on missing information or poor quality information, resulting in poor decisions. Information is not used shortly after its creation because business has forgotten the source or location of information or can't find it, resulting in cost without corresponding value.		
				Information of value is not properly secured against internal security violations or external security breaches; entities can bypass or contravene security policies, practices, or procedures. Failure in securing information deeply heightens privacy issues if information accessed is not properly protected.		
				Access, transport and use limitations are not understood by employees with information custody or collections responsibility and customers or employees rights are impacted		
				The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and disposition policy		
				Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting and disposing of information, exposing the company to significantly higher costs and risks		
				New, valuable, aging, and useless data are commingled within the data source, its back up and its non-production instances. Business users waste their time sifting through debris to find what they need without success. IT costs soar. Organization is exposed to Privacy, security and legal risks.		
				IT is unable to dispose of data and decommission systems causing significant unnecessary cost and risk; IT improperly disposes of data causing unnecessary risk and legal or business expense		
				IT is unable to associate data with business stakeholders or ensure legal duties are met, leading to oversight in collecting evidence and unnecessary legal and operating costs		
				Storage is over-allocated, misaligned with business needs and consumes unnecessary capital; IT is unable to reclaim storage and eliminate cost after data is deleted causing unnecessary cost		
				Unable to demonstrate reasonable efforts to establish and follow governance policies and procedures increases sanctions risks, penalties and judgments and erodes customer trust		

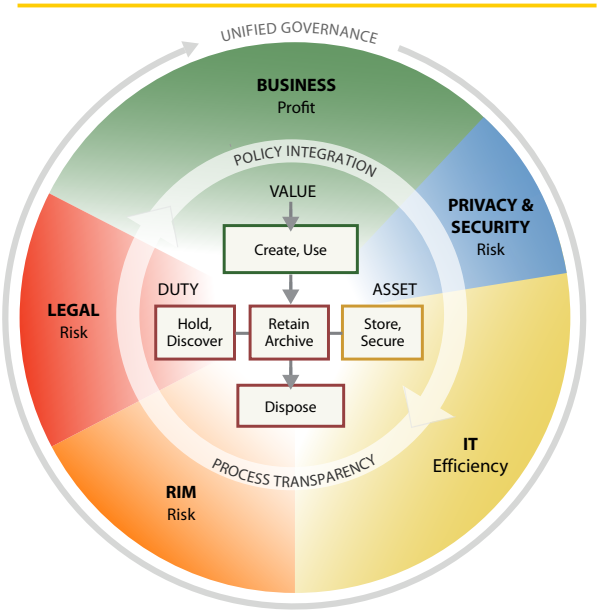
Conclusion

In a world where CEOs, CIOs, and GCs are continually challenged to drive financial performance, there's a growing imperative to take cost and risk out of business operations. An Information Lifecycle Governance program can create tremendous value for an organization by formalizing processes around defensible disposal and aiding companies in their quest to substantially improve information economics. Aligning information stakeholders, processes and practices across legal, records, privacy, business functions, and IT enables the collaboration necessary to systematically lower risk and cement ILG processes into the foundation of an organization's information management culture.

The cost and risk reductions to be gleaned from defensible disposal practices lie in stark contrast to the implications of compounding data costs and conducting business as usual. While this is intuitively obvious to corporate officers and executive leaders who clearly see the big picture and are the frequent targets of discovery requests, achieving results requires cross-functional change and a major transition from disparate, siloed practices to a joint-stakeholder model. The only way to achieve lasting information economic success, therefore, is to have a clear lifecycle governance strategy anchored in material business outcomes buoyed by a multi-level governance organization and strong program leadership.

With such far-reaching ramifications, an ILG program is an important lever for C-level executives, and it's also a significant career opportunity for ILG leaders. We hope this guide serves as deep dive into proven ILG methods and defensible disposal practices while serving as a compass to steer companies to improved information economics.

Policy and Process Integration Across Information Stakeholders Enables Disposal, Lowers Cost and Risk



Information Governance Reference Model / © 2012 / v3.0 / edrm.net

Strategy and Execution Drive Business Outcomes with Structure, Defined Processes, Metrics, Capacity & Accountability

STRATEGY

Governance Program Driving Savings and Risk Metrics
Charter, directive and accountability for enterprise program. Savings achievement cadence and reporting.

Program Office to Coordinate Stakeholders, Drive Benefit Achievement
Ensures cross-silo engagement and progress toward maturity targets and financial objectives, change management

EXECUTION

Technology Provides Capacity to Improve and Integrate Processes, Consistently and Defensibly Dispose, Decommission
Automates processes, ensures transparency, provides capacity. Accelerated deployment to drive faster save.

Reclamation Removes Excess Storage, Infrastructure
Savings-prioritized reclamation and recovery of infrastructure to drive P&L benefit

$100M enterprise value creation through lower legal and IT costs, reduced risk

About CGOC

CGOC (Compliance, Governance and Oversight Council) is a forum of over 2,900 legal, IT, records and information management professionals from corporations and government agencies. CGOC publishes reference guides and articles and conducts primary research; its Benchmark Reports have been cited in numerous legal opinions and briefs and its ILG Leaders Guide widely referenced and adopted by organizations. CGOC members convene in small working groups, regional meetings and its annual strategy summit to discuss information governance and economics, eDiscovery, data disposal, retention, and privacy. CGOC has been advancing governance practices and driving thought leadership since 2004. For more information go to www.cgoc.com.

For inquiries please contact us at cgoc@cgoc.com or go to www.cgoc.com for more information.
ILG Reference Guide — 042413V9

COURTESY OF